Symposium on the Target Breach, 
FTC v. Wyndham and Heartbleed

Overview

By
Neil J. Cohen, Publisher

“The general belief that any type of security defense can be 100% effective has come to an end. The new reality is that at least one or more systems within a given environment are most likely already compromised, and the job of IT Security is to minimize damage by discovering and neutralizing intruders after they have infiltrated the environment.”

Philip Lieberman, Lieberman Software

“For $1 million I could assemble a team that could hack into nearly any target. But $1 million wouldn’t be nearly enough for a company to defend itself.”


Since consumers are protected by the banks’ zero liability policies for fraud, what are the consumer risks of insecure cybersecurity? According to consumer credit expert John Ulzheimer, consumer names and personal information are even more important to the hacker than the credit card number:

Regarding data breach value, let’s take the Target breach for example where it appears names and email addresses have also been stolen by the tens of millions. That information, if used, will likely be used to send spear-phishing emails, which are emails that are well designed with relevant content and not simply a shotgun method of sending millions of random emails in an attempt to fool someone into replying. Spear-phishing emails will
Comments on Our Other Publications . . .

The Bank and Corporate Governance Law Reporter is a monthly publication designed to serve litigators. It includes opinions, briefs, and transcripts of oral arguments in key FIRREA, FIDICIA, and corporate governance cases. Subscribers receive articles on cutting-edge issues, analyses of cases in the context of prior law, and detailed indexes.

"The Reporter probes beneath the surface of reported opinions in major M&A cases and gives to the reader ready access to the cutting-edge arguments made by leading practitioners in the field. It is a critical tool for anyone seriously interested in staying one step ahead of developing legal trends in the area."

A. Gilchrist Sparks III
Morris, Nichols, Arsht & Tunnell

PRICE: $4175/YEAR

Many lawyers have discovered that the Chemical Waste Litigation Reporter is the most effective and comprehensive publication to obtain, organize and digest the flurry of judicial opinions in Superfund and related insurance, toxic tort and commercial cases. No other service publishes the decisions, organizes them under issue headings, and analyzes them in the context of existing case law.

"We are very pleased with your reporter and believe that it provides a very useful tool both in litigation and counseling clients in the area of hazardous waste."

Charles Tisdale, Jr.
King & Spalding

"The Reporter is an invaluable blend of published cases, briefs, news and analysis on the cutting edge of hazardous waste litigation. This publication is also a valuable research tool. Its well-organized index of relevant CERCLA provisions allows rapid identification of cases on point."

Michael A. Brown
McCutchen, Doyle, Brown & Enersen

PRICE: $3775/YEAR

Many lawyers believe that the RICO Law Reporter is the most effective and comprehensive of the civil RICO reporting services. No other service publishes the decisions, organizes them under issue headings, and analyzes significant new decisions in the context of existing case law. Such headings include Arbitration, Burden of Proof, Conspiracy, Discovery, Enterprise, Equitable Relief, Evidence, Forfeiture/Disgorgement, Jurisdiction, Pattern, Pleadings, Predicate Acts, Res Judicata, Sanctions, and Standing. Also included every six months is a Cumulative Decision Index.

"The RICO Law Reporter is more than a 200-page monthly legal newsletter. By continuously publishing timely articles and analyzing and synthesizing the published opinions, the editors have created, in effect, a first-rate civil RICO treatise, updated monthly."

Frank C. Razzano
Pepper Hamilton LLP

PRICE: $3725/YEAR

To order, call 202-462-5755

Visit us on the Web at http://www.lawreporters.com
Board of Editors

Fred M. Greguras, Esq.
K&L Gates
630 Hansen Way
Palo Alto, CA 94304

Tobey B. Marzouk, Esq.
Marzouk & Parry
1120 19th Street, N.W.
Seventh Floor
Washington, DC 20036-3605

Michael F. Mason, Esq.
Hogan & Hartson
555 13th Street, N.W.
Washington, DC 20004-1109

Gary J. Rinkerman, Esq.
Drinker, Biddle, & Reath LLP
1500 K Street, NW
Washington, DC 20005

Professor Stephen Saxby
Faculty of Law
Southampton University
Highfield, Southampton
S017 1BJ U.K.

Richard H. Stern, Esq.
Kellogg Huber Hansen Todd, Evans & Figel, PLLC
1615 M Street, NW
Suite 400
Washington, DC 20036

J.T. Westermeier, Esq.
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
11955 Freedom Drive
8th Floor
Reston, VA 20190-5675

E. Robert Yoches, Esq.
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
1300 I Street, N.W.
Washington, DC 20005-3315
will speak to you, personally, because they’ll likely include information about where you actually work, where you actually bank, where you actually went to school, or things you’ve actually purchased online. Those emails will include links leading to sites that will install malware on your computer or at least ask you to provide other valuable sensitive information. Moreover, a hacker can use your personal information to apply for things in your name including credit, insurance, employment, utilities, and medical services.

Given those risks, couldn’t the FTC play a useful role incentivizing those who would otherwise provide cheap and vulnerable protection? The article by Jay Westermeier, infra, provides an excellent summary of the FTC’s guide to “reasonable” standards for data protection based on the use of firewalls, encryption, virus detection risk assessments, employee screening and training, disposal of information, access controls, incident response plans, monitoring, investigative processes, and contractor oversight, all balanced by cost and potential harm.

Can government intervention be helpful when a software flaw like Heartbleed pervades the entire internet infrastructure? As described by Blank Rome authors in a Mondaq post on April 23 Heartbleed is:

a serious vulnerability in the popular OpenSSL cryptographic software library. OpenSSL is used by most web sites and network equipment manufacturers to convert sensitive information into a string of unrecognizable characters (i.e. encryption). Heartbleed exploits a flaw in OpenSSL to access private data such as usernames, passwords, and credit card numbers. OpenSSL is used by at least 66 percent of all servers on the internet, including popular sites such as Google, Yahoo, Amazon, Netflix and Tumbler… Originally thought to primarily impact consumers, a recent announcement by Cisco Systems and Juniper Networks, Inc. exposes Heartbleed as a major threat to corporate networks. The two largest manufacturers of network equipment stated that some of their products contain the Heartbleed bug. With the bug located on the hardware of many corporate servers, traditional defenses such as firewalls and virtual private networks may be ineffective. Hackers may now be able to exploit the flaw with hardware to infiltrate the networks and capture usernames, passwords and other sensitive information stored on corporate networks.

Will the Heartbleed bug trigger a flood of lawsuits? Probably not. The bug is so pervasive that plaintiffs’ lawyers will be hard pressed to prove that a breach was caused by corporate negligence when it could have been caused by a reverse attack from a router or by way of a flaw in the security system of a third-party service provider. In other words, plaintiffs’ lawyers will have difficulty tracing the original source of the breach and proving through their own experts or discovery that retailer negligence was its proximate cause. According to security expert Winston Krone, “Since most data breaches are the result of multiple vulnerabilities, the pervasiveness of the Heartbleed bug will make proving liability more difficult. Particularly, credentials taken using the Heartbleed
bug could be used to mount completely separate attacks on third parties – which might nevertheless be stopped if the third party has sufficient defenses in depth”.

Even if the Heartbleed bug resides on a company’s own network, and the company negligently fails to detect it, the plaintiff will not be able to prove the bug was the cause of the breach. According to security expert James Huguelet, “By the nature of the software defect underlying Heartbleed, a criminal using it for an attack almost never leaves any trace that the affected system was compromised. Because of this, it’s difficult to even know if a site has been successfully attacked and, if so, what data might have been taken. I think this will make it very, very difficult to prove that a loss of data was attributable specifically to Heartbleed, much less a specific equipment vendor’s use of OpenSSL that included the Heartbleed bug.” Since neither party can lay the blame on Heartbleed, and plaintiffs have the burden of proof, the bug should be a boon to defendants.

Nevertheless, as attorney Mauricio Paez points out, companies should correspond with third-party providers to determine if they used open SSL and if so, have they investigated for the bug, what, if anything, has been done to patch or replace defective firmware, and what information do they have about whether their system has been compromised? This advice mirrors FTC guidance on April 11 that, “If you have business partners or contractors the provide technical services or support, you also want to confer with them to address any problems in their systems.”

Even so, corporate officers may respond, “What’s inside the router is not my problem” and third-party providers may acknowledge a bug but resist a fix. According to Mr. Philip Lieberman:

Networking giant Cisco has confirmed that a number of its products are vulnerable, including desktop phones, video conferencing hardware and VPN software. . . . Most of the devices are not going to be patched because their users do not know how to do it since they bought a router or firewall, not Open SSL (as far as they are concerned). Many of the devices are from manufacturers that are not longer supporting the previously shipped devices …. What do you expect in the way of support when you buy a device or embedded system for less than $100 and the selling company is making $10.00.

If so, the FTC should impose a rule or “fairness” duty for corporations to determine whether the bug exists on third-party firmware that affect communication to and from customers. In that case, the FTC could impose a duty to change passwords to those systems or, if possible, bypass them. Similarly, the FTC could determine that vendors have a duty to recall or replace defective firmware. At a minimum, the FTC and the courts may decide that a company’s communications to customers regarding Open SSL corrections need to qualify absolute assurances by stating that the problem may not be solved, because the bug may still exist on defective software and hardware in the communication chain.
What Is the Technology Gold Standard?

Will the problem be largely solved in October 2015, the date the banks, credit card companies and merchants have voluntarily set to replace the vulnerable magnetic strip containing unencrypted information with chip-enabled smart cards called EMV? Under the new system, the credit card networks will institute a fraud liability shift, i.e., if a consumer’s card is involved in fraud, whichever party involved in the transaction (the bank that issued the card or the merchant that accepted it) that didn’t upgrade to EMV will be held accountable.

The smart card is supposed to foil hackers because each time the consumer uses it the credit card number is encrypted differently by the connection between the chip and the point of sale terminal. The chip plus pin technique, the European standard, is considered more secure because it provides two layers of encryption and makes forgery of credit cards impossible. One important reason Europe has the chip and pin standard is because it absolves the banks of liability. If the pin is used in a transaction the customer is held liable for the loss on the ground that he either made the purchase or did not properly protect his pin number. In the US Regulation E under the Electronic Fund Transfer Act of 1978 forbids this shift in liability from the banks.

According to security expert James Huguelet (see interview infra) even the chip plus pin standard is not secure enough because it does not provide “application level end-to-end encryption in motion”, whereby the card holder information is encrypted before it ever leaves the physical confines of the merchant’s PINpad, so even if a cyber attack tries to intercept it coming out of the PINPad it is already encrypted and therefore completely worthless to the cybercriminals. Mr. Huguelet says:

It is widely thought (and often reported in the media) that the implementation of a chip-based card format like EMV will encrypt consumer data while it is in motion. This is simply incorrect, as there is no requirement to encrypt critical EMV data like the account number when it is in motion.

This is a fundamental weakness in how EMV is being promulgated in the US, and the lack of this requirement is shocking and very near-sighted. Without encrypting the sensitive consumer data, merchants and others will remain vulnerable to many forms of hacking (including the one that apparently affected Target) . . .

The Target Breach

Mr. Huguelet continues:

Based upon published media reports, Target appears to have used network-level encryption to secure card holder information as it traveled the few feet between the stores’ PINPads and POS registers. After doing something (reports don’t say what) with this data, the POS register then re-encrypted the data at the network-level and sent it on to its payment processor. This is akin to the armored car service
transferring your cash between two armored cars on the way to the bank – and someone can be waiting at the transfer point. Unfortunately for Target, the cyber thieves stole the data when it was in the process of being transferred coming in from the PINPad but before it was re-encrypted and sent out to the payment processor.

The Lufthansa Heist depicted in the movie Goodfellas followed the same approach: the gang didn’t steal money while it was on the plane and they didn’t steal it from the bank. They stole it while it was being transferred from the plane on its way to go to the bank.

To be sure, some merchants are planning on implementing so-called “end to end encryption” as part of their work to become EMV-ready, but this is left solely to the discretion of the retailer.

Also amazing is the fact that implementing EMV as it is currently planned for the US will not require the use of PINs in all transaction circumstances. This is also a major compromise to the overall security promise that EMV could deliver if the card brands set the necessary rules.

Should Security Standards Be Set By the Credit Card Companies or the FTC?

Currently security standards for consumer data are set by the credit card companies and enforced by the banks that issue the cards. When a breach occurs the merchant is required to hire a contractor approved by the credit card company to determine whether the merchant was in compliance with the industry standards. If violations are found the card company imposes fines upon the bank for failing to enforce the standards that the merchant ultimately pays under an indemnification agreement.

The credit card standards are vague. Requirement number one states that the merchant is required to “install and maintain a firewall configuration to protect cardholder data.” After a breach it is impossible for the card companies not to find a breach of this requirement, thus insuring that the merchant will end up paying the bill.

The FTC’s criteria for investigating a breach is whether the merchant’s security configuration constituted a similarly vague “unfair trade practice.” When a consent decree is entered it provides for “reasonable safeguards for firewalls, encryption, virus detection risk assessments, employee screening and training, disposal of information, access controls, incident response plans, monitoring, investigative processes, and contractor oversight, all balanced by cost and potential harm considerations.

According to attorney Archis Parasharmi, “setting such standards through after-the-fact litigation conflicts with the collaborative approach that created the Cybersecurity Framework and the adoption of risk-based cybersecurity practices that it is intended to encourage. The problem with a litigation-focused approach to data security is that it is more likely to promote static security
checklists and a one-size-fits-all approach to data security, when—as recent events on the ground suggest—what is really called for is a nimble and flexible approach to fighting cybersecurity threats. By seeking to impose liability through second guessing with the benefit of hindsight, cybersecurity litigation can be expected to dampen, rather than encourage, risk-based decision making by businesses.”

But the credit card companies have little incentive to require gold-standard security from their merchants because their standard contract shifts nearly all the liability for breaches of its security standards to the card-issuing banks, and the banks require indemnification from the merchants. If the card companies, in their sole discretion, determine that there has been a breach of the firewall they can assess fines and penalties from the banks even if no actual money was stolen from the cardholders’ accounts. See *Genesco v. Visa*, No. 3:13-0202 (M.D.Tenn) where the merchant, as assignee and subrogee of the banks, challenged Visa’s claim that $13 million in fines and assessments were due because the merchant was in violation of Visa’s security standards. Genesco also claims that Visa was unjustly enriched by collection of the $13 million fine from the banks because no money was stolen from the cardholder accounts.

When I asked Mr. Huguelet whether he thought the FTC should issue a rule he said:

As a general rule, I don’t favor regulation in the payments area – even when such regulation would help set a direction for everyone in the industry to follow. The card brands should really have been able to lead the industry in setting a holistic set of standards with an associated realistic timeline for their implementation that meaningfully make the payment system more secure. That being said, my rules would be as follows:

- All credit and debit cards in issuance must be EMV capable and all merchants must be able to accept these cards.
- Magnetic stripe technology can no longer be used for credit or debit cards and merchants can no longer utilize magnetic stripe technology to accept payments.
- All credit or debit transactions would require the user to enter a PIN as part of the transaction.
- All credit or debit transactions must encrypt all sensitive cardholder data beginning within the device they are presented to for purchase (i.e., the PINPad) and continuing until they reach the merchant’s payment processor or payment switch.
- Card brands cannot contractually require merchants to retain any card holder data after a transaction is completed (i.e., for dispute or “chargeback” handling), instead providing a one-time-use token back to the merchant when a link back to the transaction is required for legitimate business purposes.
• All card brands must provide a method for e-commerce consumers to enter any necessary card holder data using a web site or other technology that is solely under their absolute control (and not the e-commerce merchant’s), providing a one-time-use token back to the e-commerce merchant to use in place of the card holder data.

• All of the above would take place no sooner than 2020.

When I asked Visa and Mastercard to respond to Mr. Huguelet they declined the invitation. In view of the sophistication hackers have exhibited, the public deserves to know why the credit card companies do not require merchants to adopt the data security gold standard. Is it because the credit card companies have made a deal with the NSA to leave a transparent backdoor so NSA can see whether suspected terrorists are using their credit cards to purchase explosives?

The FTC should hold hearings to determine whether it should issue a rule based on Mr. Huguelet’s recommendations, whether the banks, credit card companies or FTC should enforce it and whether the card companies or the government should receive the fines for a breach of the standards.

In the meantime, what is the anxious consumer to do? One can change passwords and change from debit to credit cards. But after a credit report reveals you have an identity thief twin the best upgrade may involve credit cards, a trashcan, pocket cash and a checkbook.
What is the Gold Standard for Data Protection Technology and Would It Have Made Target’s Credit Cards Secure From Hackers?

Publisher’s Interview of James Huguelet, President of the Huguelet Group LLC

Q. Jim, you stated to Computerworld that real protection for credit cards means “end-to-end encryption in motion”? Please explain what that is and how it could have provided protection for Target’s customers?

A. There are two approaches to encryption, both of which are often called “end to end,” but one of which is vastly more secure than the other. Understanding the difference between network-level (sometimes called “transport-level”) encryption and application-level encryption is a bit challenging for non-IT professionals, so an analogy is often useful. Imagine for a moment that you own a store, and each day you gather up in your office all of the cash customers gave you that day and want to deposit it in your bank. To do this, you hire an armored car service to safely transport that money between your store and your bank. So, every day you take the cash from your office, walk outside to meet the armored car driver, hand the cash to him, and then he drives the cash to your bank where he hands it to a teller at the bank. If someone tries to take your money while on the road to the bank, you can rest easy because it is protected by the armored car. This is akin to network-level encryption—it secures the transportation of your data from one “end” (in front of your store) to another “end” (your bank).

There’s a fundamental weakness to this approach, though. What happens if on the way between your office and the armored car (or, on the other side, the armored car and bank teller), someone is waiting and decides to take your money? The armored car isn’t there to protect you because your cash isn’t in it yet (or anymore).

* * Mr. James W. Huguelet, PMP is president of The Huguelet Group LLC, a provider of strategic information technology consulting and project management services. Prior to his work with The Huguelet Group LLC, James was the chief information officer of Aquascape, Inc., the largest manufacturer and distributor of products used in the construction of residential water features in North America. Before this role, Mr. Huguelet held a variety of director-level positions in sales, product development, and consulting management at a venture capital-backed software products and consulting company. As an industry expert in the field of electronic payments security, Mr Huguelet speaks regularly at industry conferences, including the SIGMA Executive Leadership Conference & Annual Meeting, the VeriFone Retail Payments Conference, and the National Association of Convenience Stores Annual Conference. His insights on the information technology industry have appeared frequently in national publications such as CIO, Computerworld, and PM Network.
In contrast, let’s imagine that while the cash was in your office you put it into an unbreakable strong box which only you and the bank had keys to open. You then walk outside to the armored car, hand the driver that strong box, and the driver takes the box to the bank and hands to the teller (who takes the box back into the vault to open with their copy of the key). That’s akin to application-level encryption—you are securing your data before it even leaves one “end” (your store) and doesn’t decrypt it until you are within the other “end” (the bank vault). Now, if someone robs you as you walk between your store and the armored car, it doesn’t matter—the cash is already in the strong box and it cannot be opened, so the theft yields the robbers nothing they can use.

It is this second, application-level type of “end to end encryption” that I believe needs to be implemented by the industry. In this approach the card holder information is encrypted before it ever leaves the physical confines of the merchant’s PINpad, so even if a cyber attack tries to intercept it coming out of the PINpad it is already encrypted and therefore completely worthless to the cybercriminals. In practice it’s even more secure than that, as PINPads are now built to have the reading of data and encryption occur within a single, discrete part of the PINPad which will permanently disable itself if someone tries to tamper with it to get at its data. As a result a thief cannot even access the card holder information from any other components of the PINPad itself.

This distinction can make a big difference. Based upon published media reports, Target appears to have used network-level encryption to secure card holder information as it traveled the few feet between the stores’ PINPads and POS registers. After doing something (reports don’t say what) with this data, the POS register then re-encrypted the data at the network-level and sent it on to its payment processor. In my analogy, this is akin to the armored car service transferring your cash between two armored cars on the way to the bank—and someone can be waiting at the transfer point. Unfortunately for Target, the cyber thieves stole the data when it was in the process of being transferred coming in from the PINPad but before it was re-encrypted and sent out to the payment processor.

The Lufthansa Heist depicted in the movie *Goodfellas* followed the same approach: the gang didn’t steal money while it was on the plane and they didn’t steal it from the bank. They stole it while it was being transferred from the plane on its way to go to the bank.

**Q. Do you believe end-to-end encryption would have prevented the Target breach even if the access to Target were gained through a third-party vendor or a Heartbleed bug in a router?**

**A.** Based upon published media reports, the hackers did apparently gain access to the in-store network via a third-party HVAC vendor that somehow had been granted that access
(intended by Target or not). This in and of itself would not have been a critical problem for Target, except that the hackers then used that access to break into the POS Registers and then planted sophisticated software on the POS registers that watched what happened in the memory of the POS Register. That in and of itself would not have been a critical problem, except that they apparently only used a network-level end-to-end encryption approach (technically, they used a pair of “point-to-point network-level encryption” approaches but I don’t want the explanation to get more complicated than it already is!—so when the data came from the PINPad into the POS Register and was momentarily decrypted before being re-encrypted on its way to the payment processor, the malware in memory copied and stored the card holder information. That data was then shipped out to the criminals at a later time. Had Target used application-level end-to-end encryption starting at the PINPad, the data would have still been encrypted in the memory of the POS Register and thus would have been useless to the criminals.

Without getting too deep into technical explanation and making too many assumptions about Target’s infrastructure (of which I have no direct knowledge), an application-level end-to-end encryption approach like what I propose would almost assuredly not have been affected by Heartbleed—because by the time the data ever saw any router or other network infrastructure, it would already been safely encrypted.

Q. The credit card companies and merchants are planning to phase out magnetic strip technology with embedded-chip smart cards beginning in October 2015. Will that solve the problem?

A. It is widely thought (and often reported in the media) that the implementation of a chip-based card format like EMV will encrypt consumer data while it is in motion. This is simply incorrect, as there is no requirement to encrypt critical EMV data like the account number when it is in motion.

This is a fundamental weakness in how EMV is being promulgated in the US, and the lack of this requirement is shocking and very near-sighted. Without encrypting the sensitive consumer data, merchants and others will remain vulnerable to many forms of hacking (including the one that apparently affected Target). To be sure, some merchants are planning on implementing so-called “end to end encryption” as part of their work to become EMV-ready (I’m working with a large restaurant chain now doing just this), but this is left solely to the discretion of the retailer.

Also amazing is the fact that implementing EMV as it is currently planned for the US will not require the use of PINs in all transaction circumstances. This is also a major
compromise to the overall security promise that EMV could deliver if the card brands set the necessary rules.

There are other issues with EMV implementation that are not specifically related to data in motion, such as:

- There is a real, practical issue related to debit processing “application IDs” that has not be resolved by the card brands and the approx. 20 major debit networks. Until this issue is clearly resolved, no one (with the notable exception of Walmart and, as of this week, apparently Target) is anxious to move forward with only credit-only partial solution. This was not an issue for any other region of the world that has implemented EMV, due to the centralized banking and payment regulatory authorities in those countries that do not have an equivalent in the US. Even the Fed does not have the legal authority to mandate the type of industry-wide solution that is required.

- Further complicating debit, there is a separate question as to whether implications from Judge Leon’s decision last summer on the Fed’s implementation of the Dodd-Frank “Durbin Amendment” could impose routing requirements that were never contemplated as part of the EMV application architecture. Although a federal appeals court recently overturned Judge Leon’s decision, whether the plaintiffs will appeal that ruling remains unclear. Until this issue is authoritatively resolved, no one is anxious to move forward with the possibility that substantive new debit-related requirements could manifest themselves via the courts in the next couple of years.

- Implementing EMV as it is currently planned will continue to have a magnetic stripe be available on the card - a major weakening in the overall security approach.

- Even if all of the above were to be magically solved, EMV alone does nothing to make on-line fraud more difficult. This is because a consumer will still have to type a card number into e-commerce web sites -where it is susceptible to all sort of PC-resident malware. And, card data would still be traversing the systems of the untold number of e-commerce sites throughout the US- any of which could be breached (and would immediately become a greater focus of criminals upon EMV implementation, as they have in, say, the U.K.).

**Q. If you were Chairman of the Federal Trade Commission What Rule Would You Want Implemented for Maximum Credit Card Security?**

**A.** An excellent question. As a general rule, I don’t favor regulation in the payments area—even when such regulation would help set a direction for everyone in the industry to follow. The card brands should really have been able to lead the industry in setting a
holistic set of standards with an associated realistic timeline for their implementation that meaningfully make the payment system more secure. That being said, my rules would be as follows:

- All credit and debit cards in issuance must be EMV capable and all merchants must be able to accept these cards.
- Magnetic stripe technology can no longer be used for credit or debit cards and merchants can no longer utilize magnetic stripe technology to accept payments.
- All credit or debit transactions would require the user to enter a PIN as part of the transaction.
- All credit or debit transactions must encrypt all sensitive cardholder data beginning within the device they are presented to for purchase (i.e., the PINPad) and continuing until they reach the merchant’s payment processor or payment switch.
- Card brands cannot contractually require merchants to retain any card holder data after a transaction is completed (i.e., for dispute or “chargeback” handling), instead providing a one-time-use token back to the merchant when a link back to the transaction is required for legitimate business purposes.
- All card brands must provide a method for e-commerce consumers to enter any necessary card holder data using a web site or other technology that is solely under their absolute control (and not the e-commerce merchant’s), providing a one-time-use token back to the e-commerce merchant to use in place of the card holder data.
- All of the above would take place no sooner than 2020.

I believe the above would comprehensively and holistically address all major aspects of payment processing security. From that point on, hackers would be forced to try to compromise either the physical PINPads or the systems of payment processors or card brands (which are all run by companies specializing in security). This would make the US payment system truly more secure and, given the high costs of moving to EMV in any partial way or manner, would only incrementally add to the cost of what is currently planned.
Fifty FTC Data Breach Consent Decrees Reveal the Agency’s Approach

by

J. (“Jay”) T. Westermeier*

My comments relating to the recent FTC v. Wyndham Worldwide Corp. district court ruling and the heartbleed bug are below. I will first discuss the importance of the Wyndham case in the evolution of legal liability standards applicable to information security programs and practices. Then I will address the heartbleed bug.

The FTC Information Security Cases

Today information security has become a critical legal issue, and effective information security programs have become a legal necessity. In this regard, the Federal Trade Commission has contributed significantly to defining the scope and extent of the “legal” obligations company’s must establish to implement and maintain comprehensive information security programs. In these FTC information security cases the FTC entered into a Consent Order with the respondent company requiring the company to establish, implement and thereafter maintain a “comprehensive information security program” that is “reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers.” In these Consent Orders the FTC requires that the respondent company’s information security program “contain administrative, technical and physical safeguards appropriate to the respondent’s size and complexity, the nature and scope of respondent’s activities and the sensitivity of the personal information collected from

*J. (“Jay”) T. Westermeier is Of Counsel at Finnegan, Henderson, Farabow, Garrett & Dunner, LLP resident in the firm’s Reston, Virginia office. He is past president of the International Technology Law Association (formerly known as the Computer Law Association); Life Fellow, American Bar Foundation; 2001 Burton Award for Legal Achievement and only lawyer to receive the Association of Information Technology Professionals Distinguished Information Sciences Award; serves on the Board of Editors for the *Computer Law Reporter* and *Internet Law & Business* and other advisory boards; and is U.S. correspondent for Computer Law Review International. He is listed in Intellectual Asset Management magazine’s “IAM300-The World’s Leading IP Strategists” (2009-2012); Top Attorneys in Virginia (Intellectual Property; Richmond Magazine; 2011-2013); Top Attorneys in Washington, D.C. (Intellectual Property, DC Magazine; 2011-2013); Chambers USA; America’s Leading Lawyers for Business (Intellectual Property; 2011-2012); The International Who’s Who of Internet, e-Commerce and Data Protection Lawyers (2009-2012); International Who’s Who of Information Technology Lawyers (2013); Best Attorneys in America (Information Technology; 2001-2014); Best Attorneys in Virginia (Best Lawyers; 2013); Best Attorneys in Washington, DC (2013); Virginia Super Lawyers (Intellectual Property; 2006-2012); Washington, D.C., Super Lawyers (Intellectual Property; 2007-2013); Super Lawyers Corporate Edition of Top Attorneys in Business Services (Intellectual Property; 2007-2012), The International Who’s Who of Business Lawyers (2008-2013); The Legal Eagles Most Respected in the Commonwealth of Virginia as published in Virginia Living (April 2012); rated “AV Preeminent” for 2013 by Martindale-Hubbell for excellence in both legal ability and ethical practice; and many other lists of distinction. Jay is a West Point graduate. In addition to his BS from the U.S. Military Academy, he has an MBA and LLM from George Washington University and a JD from American University, where he served on the law review. He also has been certified by the Institute for the Certification of Computer Professionals as a Certified Computer Professional. In addition to his counseling and transaction practice, he serves as a legal expert witness, arbitrator and mediator, and litigates in federal and state courts.
or about consumers.” The FTC has issued Consent Orders in approximately 50 information security cases. These FTC consent order cases help to set the minimum legal standards for information security. They define adequate security to mean that companies maintain effective security that is commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, impairment, modification or destruction of information. These FTC information security consent order cases are extremely important to the legal community. That’s why the district court’s ruling in FTC v. Wyndham Worldwide Corp., Civil Action No. 13-1887 (ES) (D. New Jersey April 7, 2014), is so important to the evolution of the legal liability standards applicable to information security.

The Wyndham ruling denies Wyndham’s challenge to FTC’s authority to assert claims under Section 5(a) of the FTC Act in the data-security context. In so ruling, the district court holds that the FTC has the authority to assert information security unfairness claims even though the FTC has not promulgated information security regulations and also finds that the FTC’s allegations regarding Wyndham’s inadequate information security practices, as a whole, were sufficient to plead viable information security unfairness and deception claims under Section 5(a) of the FTC Act. As such, the district court ruling strengthens the legal underpinning for all of the FTC’s information security consent orders.

The Wyndham complaint follows the FTC’s typical complaint in the information security Consent Order cases. The FTC alleges the breach damages then identifies the inadequate practices that, taken together, allowed the unauthorized access and theft, and caused damages to consumers. The FTC alleged that, since April 2008, Wyndham “failed to provide reasonable and appropriate security” “by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.” As a result of these failures the FTC alleged three breaches occurred where intruders gained unauthorized access to Wyndham’s computer network, including Wyndham’s property management systems. Based on these information security breaches the FTC alleged more than 619,000 consumer payment card accounts were compromised, and many of those account numbers were exported to a domain name in Russia, with fraudulent charges on many consumers’ accounts and more than $10.6 million in fraud loss.

The district court in the Wyndham case concluded that the Wyndham defendants’ insufficient information security practices, in the aggregate, caused the data breaches that resulted in the losses. The court discussed Wyndham defendants’ insufficient practices that permitted the unauthorized access to occur. The discussion of these insufficient practices provides important, instructive information and guidance regarding comprehensive information security programs. Courts have considered these FTC security cases in finding unfair and deceptive practices under state law. See, e.g., In Re TJX Companies Retail Security Breach Litigation, 564 F.3d 489 (1st Cir. May 5, 2009);
In Re Hannaford Bros. Co. Customer Data Breach Litigation, 2009 W.L. 325056 (D. Me. May 12, 2009). It is hoped that companies will implement and maintain comprehensive information security programs with these FTC consent order cases and the Wyndham case in mind. But companies are not required by law to implement comprehensive information security programs, unless they are subject to a consent order.

Insufficient Practices

While the Wyndham case does not assess liability against the Wyndham defendants, the ruling does identify a number of allegedly insufficient information security practices by the Wyndham defendants in connection with assessing the sufficiency of the FTC’s complaint allegations. It is these insufficient practices that are identified that make the Wyndham case and the FTC information security consent order cases so valuable. These insufficient practices relate to password management, use of firewalls, use of encryption, virus detection, risk assessments, employee screening and training, disposal of information, access controls, incident response plans, monitoring, investigative processes, contractor oversight and other insufficient practices.

Generally, risk assessments based on these cases are viewed from a reasonable cost perspective. Where proven security controls were available at a relatively low cost, the FTC found the company had failed to protect information security adequately, especially where the FTC believes the risk should have been foreseeable. Severity of the risk, foreseeability, cost and reasonableness are all important criteria in assessing the sufficiency of information security practices. What is reasonable for a particular company will vary based, among other factors, upon its size and complexity, the nature of its business, and the sensitivity of the information it collects. This is a major obstacle to enacting legislation applicable to all companies because the risks and other factors vary from company to company. The Wyndham case and other FTC consent order cases identify many different “insufficient practices”. Some of those insufficient practices are discussed below.

Password Management

One key aspect of access controls is password management. The FTC alleged that the Wyndham defendants “failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess” and “did not require the use of complex passwords for access to the Wyndham-branded hotels’ property management systems and allowed the use of easily guessed passwords.” The FTC has emphasized password management in other FTC consent orders. For example, in the Matter of Twitter, Inc., FTC File No. 092-3093 (June 24, 2010), the FTC’s Complaint alleged that Twitter failed to provide reasonable and appropriate security to prevent unauthorized access to non-public user information by, among other practices, failing to “establish or enforce policies to make administrative passwords hard to guess, including policies that: (1) prohibit the use of common dictionary words as administrative passwords, or (2) require that passwords be
unique – i.e., different from any password that the employee uses to access third-party programs, websites, and networks. “In the Twitter case other insufficient password management practices included the failure to: (1) “establish or enforce policies sufficient to prohibit storage of administrative passwords in plain text in personal email accounts”, (2) suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts, and (3) change passwords periodically, such as by setting administrative passwords to expire every 90 days.

**Firewalls**

Another aspect of access controls is firewalls. In the Wyndham case the FTC alleged that the Wyndham defendants had failed to use firewalls to limit access to their computer systems. The failure to use firewalls has been noted in a number of the FTC information security consent order cases.

**Encryption**

One of the most important strategies relates to encryption of data in storage and in transmission. One of the deficiencies alleged against the Wyndham defendants related to permitting “storage of payment card information in clear readable text.”

**Network Management**

In the Wyndham case, the FTC alleged that the Wyndham defendants failed to inventory the computers connected to the hotel network so they could not manage their network. In addition, the FTC alleged the Wyndham defendants permitted Wyndham-brand hotels “to connect insecure servers, including servers using outdated operating systems for which security updates or patches to address known security vulnerabilities could not be installed.

**Monitoring**

The FTC alleged the Wyndham defendants failed to monitor the hotel’s computer network for malware used in a previous intrusion. The FTC has found the failure to intrusion detection systems to be an insufficient practice.

**Access Controls**

In the Wyndham case, the Wyndham defendants were alleged to have used insufficient access controls.

**Virus Detection Software**

The failure to use updated, current virus detection software has been found insufficient. It is important to install new releases to virus detection software.
Disposal of Information

In the Matter of Rite Aid Corporation, FTC File No. 0723121 (July 27, 2010), is an example where the FTC filed a Complaint and entered into a consent order against Rite Aid for discarding materials containing personal information in clear, readable text in unsecured, publicly-accessible trash dumpsters used by Rite Aid.

Training and Employee Screening

There are many FTC consent order cases where the defendant respondent failed to train employees to handle information securely. Other consent orders identify employee screening.

System Configuration

The FTC has noted that critical systems that do not require connectivity should be isolated to reduce the risks resulting from connectivity.

Web Attacks

Numerous FTC consent order cases found the respondent had not adequately assessed the vulnerability of their web application and network to commonly known or foreseeable attacks, such as “Structured Query Language” (“SQL”) injection attacks; and did not implement simple, free or low-cost, and readily available defenses to such attacks.

Third Party Access

Other FTC cases addressed the failure to assess the risks relating to third party access and to employ sufficient measures to detect and prevent unauthorized access.

Security Investigations

The FTC has also alleged that respondents have failed to conduct security investigations following up on security warnings and intrusion alerts.

Contract Providers

Another area is where third-party service providers are not required by contract to protect the confidentiality and security of personal information.

Updating Programs

The FTC has alleged that respondents have failed to evaluate and adjust their information security programs in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.
Incident Response Plans

The FTC has also alleged inadequate incident response plans and measures to minimize any losses.

Critique of FTC Jurisdiction

The use of Section 5 of the FTC Act to develop information security law through consent order cases and adjudicated cases is a very indirect and slow road to requiring companies to adopt, use and maintain comprehensive information security programs. A more direct statutory enforcement program is needed. Specific laws dealing with specific information security practices, procedures and policies should be enacted.

That said, enacting an appropriate law or laws is very difficult. Technology is constantly changing. Hackers become more sophisticated every day. Information security needs to be comprehensive and be continually strengthened and improved based on continuous risk assessments. Risk assessments must be performed on a continual basis.

Companies should identify reasonably foreseeable material risks, both internal and external, to the security, confidentiality and integrity of information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and do an assessment of the sufficiency of any safeguards in place to control those risks. At a minimum, the risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures. The employee training risks should include the risks posed by lack of training and failure to screen employees.

The Section 5 FTC cases focus on personal consumer information rather than protectable information generally. In some respects, this is a deficiency because the FTC cases do not define insufficient information security practices, procedures and policies for all forms of protectable information.

Developing acceptable information security legislation is very difficult but needs to be developed and enacted.

Heartbleed Bug

Many believe open source software offers more flexibility and security than proprietary code because the code is available for inspection. However, the Heartbleed bug shows that even with the transparency of open source software, bugs can be missed and overlooked.
The Heartbleed bug occurred in the Open SSL cryptographic software library. This vulnerability is very serious. It permits the theft of information including secret keys, the names and passwords of users, and actual content protected by SSL/TLS encryption.

The Heartbleed bug is malware even if it was developed by accident. Accidental bugs may do just as much harm as an intentionally released computer virus. Code inspection needs to be complete. By most accounts, it took far too long to identify and develop a remedy for the Heartbleed bug which allowed computer hackers to take advantage of the bug to attack systems and established controls. It was introduced to the Open SSL code in December 2011, but was not made public until April 8, 2014.

Open source software is not risk free. Agreements need to contemplate potential problems even with open source software. Preventive, risk-management information needs to be disseminated widely and expeditiously so that the losses from a bug like the Heartbleed bug can be implemented promptly by everyone. Incident response plans need to contemplate bugs like the Heartbleed bug.

I believe liability for the heartbleed bug will depend on the reasonableness and timeliness of the actions taken to identify the bug and prevent any further harm to companies, their customers and connected third parties.

With the bug located on the hardware of many corporate servers, companies should consider using open source scanning tools such as Black Duck to identify Open SSL Code integrated throughout their infrastructure so that the code may be identified and fixed quickly. Apparently, the fix is relatively easy to install. The scanning software may be the fastest way to identify the Open SSL Code.

I believe that data breach notifications are likely to be required by many companies who believe they may have been breached as the result of the heartbleed bug. Forty-six states have data breach notification statutes. Companies will need to determine whether compliance with applicable breach notification laws is appropriate.
Wyndham, Heartbleed, and the Pitfalls of Setting Cybersecurity Standards Through Litigation

by

Archis A. Parasharami & Stephen Lilley*

In the world of data breaches and cybersecurity, 2014 has already been an eventful year before it is even half over. In recent weeks, the Heartbleed bug has launched hundreds of headlines, if not more—following on the heels of reports of one high-profile breach after another.¹ In the wake of these reports, mitigation costs for companies victimized by network intrusions and data breaches are continuing to soar.² And (inevitably) litigation has sprung up at every turn, seeking to impose liability for alleged violations of data-security standards that, in our view, have been discovered post hoc and with little regard for the defendant’s cybersecurity efforts.

All of these developments have taken place against the backdrop of a continuing debate about how the nation should respond to the potentially severe cybersecurity-related threats to its national and economic security as well as to sensitive personal and business information. On one point, however, there is a growing consensus: Nearly everyone agrees that our national strategy must include a public-private partnership for the development of broadly applicable cybersecurity standards. This view—reflected in the recently-announced National Institute for Standard and Technology’s Cybersecurity Framework³—recognizes that the private and public sectors must work together to strengthen our nation’s cybersecurity. It likewise recognizes that one-size-fits-all checklists are inferior to risk-based cybersecurity practices, and that real-time cooperation is vastly superior to rigid regulation that can rapidly (perhaps instantly) become obsolete. Thus, an ever-expanding group of stakeholders share the common goal of leveraging market forces—whether through insurance contracts, investor demands, or customer/vendor requirements—to ensure that all companies have appropriate cybersecurity practices and procedures aimed at mitigating the risks that they face.⁴

By contrast, the value of regulation-by-litigation in response to cyber incidents and threats is far less clear. Indeed, whether such matters belong in court at all has (appropriately) proven to be

* Archis A. Parasharami is a litigation partner in Mayer Brown’s Washington, D.C. office and co-chair of the firm’s Consumer Litigation and Class Action Practice. Stephen Lilley is an associate with the firm.

¹ See, e.g., Jim Finkle, Little Internet Users Can Do to Thwart ‘Heartbleed’ Bug, Reuters (Apr. 9, 2014).


a significant threshold question. Countless putative class actions have been brought by plaintiffs asserting claims about data breaches, large and small. These lawsuits are not filed against the unknown hackers, of course, but instead against the companies that themselves were victimized. But courts often reject these lawsuits for lack of standing, because plaintiffs frequently fail to allege or demonstrate that they have suffered any particularized injury (as opposed to a general heightened fear of identity theft).  

Nonetheless, not every such case is dismissed for lack of standing, and recent developments suggest that these lawsuits may become even more common. One potential trigger: In the closely-watched Wyndham case, a federal district court recently held that the Federal Trade Commission (FTC) may use its broad and vague “unfairness” authority under Section 5(a) of the FTC Act to enforce data-security standards. This move is likely to encourage further FTC enforcement actions and follow-on private litigation. But whether such litigation will be common and whether it will be a good idea—more specifically, whether setting de facto standards through FTC enforcement actions or private class actions is wise cybersecurity policy—are two different questions.  

In our view, the use of litigation in response to data breaches and other cyber incidents is highly unlikely to identify and drive the adoption of constructive cybersecurity standards. To the contrary, setting such standards through after-the-fact litigation conflicts with the collaborative approach that created the Cybersecurity Framework and the adoption of risk-based cybersecurity practices that it is intended to encourage. The problem with a litigation-focused approach to data security is that it is more likely to promote static security checklists and a one-size-fits-all approach to data security, when—as recent events on the ground suggest—what is really called for is a nimble and flexible approach to fighting cybersecurity threats. By seeking to impose liability through second guessing with the benefit of hindsight, cybersecurity litigation can be expected to dampen, rather than encourage, risk-based decision making by businesses.

The Wyndham Case

The Wyndham action arose when a group of hackers allegedly penetrated the hospitality chain’s networks from 2008 to 2010, thereby compromising over a half-million payment card numbers. Wyndham, which already faced a substantial prospect of financial and reputational harm caused by the hackers’ crime, next found itself facing a civil action filed by the FTC. In that lawsuit, the FTC alleged that Wyndham had not maintained reasonable and appropriate data-security measures.  

The agency claimed that Wyndham had engaged in (1) deception through alleged misrepresentations


of the company’s data-security practices; and (2) “unfair” conduct based upon the harms allegedly suffered as a result of the purportedly unreasonable data-security practices.

Wyndham moved to dismiss the amended complaint, arguing, among other things, that the FTC’s “unfairness” authority does not extend to data security, that the FTC had failed to provide fair notice of what Section 5 of the FTC Act requires, and that Section 5 does not govern the security of payment card data. Wyndham—joined by a number of amici—pointed to the FTC’s lack of clear statutory authority, the continued legislative debates about data-security standards, and the FTC’s failure to establish standards through rulemaking as powerful reasons why the FTC lacked the authority to regulate data-security practices through Section 5 enforcement actions.

The district court was not persuaded. It concluded that more narrow data-security requirements enacted by Congress complemented, rather than precluded, the FTC’s assertion of authority under Section 5. The court also disagreed with defendants about the import of the ongoing legislative debates and prior statements by the FTC about the limits of its authority to regulate data security. The court thus declined “to carve out” what it understood to be “a data-security exception to the FTC’s authority.” The court likewise held that the FTC did not need to promulgate rules before exercising that authority, and that the FTC had adequately pled its unfairness claim. Finally, the court rejected the defendants’ challenge to the FTC’s deception claim.

As a result of the Wyndham decision, companies can expect the FTC to continue—and perhaps even expand—its efforts to regulate data-security standards through enforcement actions. Indeed, many observers believe that the district court’s decision—and the resulting headlines—may serve to boost the FTC’s efforts to regulate data security. This change will have at least three significant negative effects.

First, past FTC actions have spawned follow-on class litigation. Continued or possibly expanded FTC activity in the field of data security thus does not bode well for companies that must defend themselves first from hackers and then from regulators and plaintiffs’ attorneys who seek

---

10 Id. at *5-9.
11 Id. at *4.
12 Id. at *15-16.
13 Id. at *25.
to turn a company’s victimization into a basis for claimed liability. Likewise it ensures that further resources will be diverted away from cyberthreat risk-management and instead directed towards managing against the risk of litigation.

Second, the district court’s highlighting of what it called “data-security insufficiencies” foreshadows a focus on simplistic checklists rather than on risk-based data-security practices.\footnote{See id. at *19.} These supposed “insufficiencies” include allegations that the company stored unencrypted data, used outdated operating systems, and failed to require the use of complex passwords. These purported “insufficiencies” were described in a manner bereft of any context—and in particular, without any reference to the specific risks facing the company or the company’s overall security response. Yet data security is not one-size-fits-all. Context does matter: every network and associated risk profile is different, and a company’s cybersecurity posture cannot be simplified down to a handful of technological decisions.\footnote{See NIST, Cybersecurity Framework v. 1.0, at 2 (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (“The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary.”).} For that reason, the creation of a data-security checklist through litigation, whether by the FTC or by a putative class representative, will benefit no one.

Third, the district court’s willingness to authorize case-by-case development of data-security standards—including through the use of consent orders that provide little or no guidance to non-parties—promises legal and regulatory uncertainty for companies in an area that cries out for stable and predictable guidelines. This uncertainty will only increase if class actions are allowed to further complicate the existing patchwork of data-security standards.

At bottom, the *Wyndham* decision is troubling for companies that seek to manage data-security risks and stave off unnecessary and inappropriate litigation. Indeed, the district court appeared resigned to the prospect of more litigation in this area, noting that “we live in a digital age that is rapidly evolving” and that will raise “a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future.” Companies certainly should hope that the district court was wrong to forecast more litigation, but should be prepared for continued legal uncertainty and the opportunistic litigation it will generate. We should not have high hopes that improved data security will follow.

### The Heartbleed Bug

If the decision in *Wyndham* is a bombshell in the world of cybersecurity law, the recent (and widespread) news of the Heartbleed bug set off fireworks of its own in the technological arena. The origins and operation of the Heartbleed bug have been well catalogued.\footnote{See generally Brian Krebs, Krebs on Security, ‘Heartbleed’ Bug Exposes Passwords, Web Site Encryp-} In short, it is a vulner-
ability in the widely-used open source Secure Sockets Layer (SSL) encryption protocol that can allow a hacker to access the information stored on a device using that technology. This vulnerability is significant since that information may include encryption keys, passwords, or other sensitive information.

A few basic points about the Heartbleed bug merit emphasis. First, the vulnerability is a simple one, as are the techniques for exploiting that vulnerability. Second, to the extent that the Heartbleed vulnerability was not exploited by hackers, it was because the vulnerability remained undiscovered, unlike other “zero day vulnerabilities” that are traded on a thriving black market. Third, because of the broad use of the SSL technology, the Heartbleed vulnerability found its way into an enormous number of websites, as well as pieces of hardware, resulting in significant remediation challenges and expense. Thus, the Heartbleed bug was one that companies likely could and would have protected their networks against—*if* they had they known about the vulnerability—but that now imposes significant remediation challenges because of how long the vulnerability was unrecognized.

But should litigation play any role in addressing such a vulnerability? In our view, the answer is no: the Heartbleed bug, arriving on the heels of the *Wyndham* decision, provides a compelling example of why FTC enforcement actions and private litigation are unlikely to improve cybersecurity standards.

As noted above, though the Heartbleed bug was simple, “reasonable security procedures” could not be expected to identify any exploitation of this vulnerability, or even the vulnerability itself. In our view, a company’s data-security practices cannot be deemed unreasonable—and the FTC thus cannot state an unfairness claim—simply because of such an unknown vulnerability that was shared by large numbers of sophisticated online merchants as well as providers of email and countless other popular services. Conversely, “reasonable security procedures” cannot be expected to prevent the most sophisticated hackers, using the most advanced tools, from penetrating a company’s networks. Thus, the FTC’s “unfairness” authority should apply only to a limited set of instances, from which unknown threats and highly sophisticated threats ought to be excluded.

These limitations call into question the out-sized role that the FTC has claimed with respect to data-security law and policy. The FTC should be very careful not to exercise this asserted authority in a way that causes companies to prioritize cybersecurity resources towards fending off litigation risks and away from the broad swath of cyber risks to which the FTC does not speak. Companies should be working collaboratively and in real-time with the federal government and each other to respond in a risk-based manner (not a litigation-avoidance-based manner) to the full set of threats.

---

facing their networks. They should not constantly have to look over their shoulders or read the tea leaves of past FTC actions for fear of being second guessed by the FTC.

The Heartbleed bug likewise demonstrates the limitations of class-action litigation in the data breach context. Given the widespread use and industry acceptance of the open source SSL protocol, private plaintiffs would likely fail to state a claim for negligence or failure to meet standards of commercial reasonableness (or any other standard other than strict liability, for that matter). It is not reasonable to expect that any company should have made itself immune to the Heartbleed bug before it was discovered and publicized. For the most part, then, it seems unlikely that class actions launched over the Heartbleed bug will gain much traction, although perhaps some plaintiffs’ lawyers will try.

In our view, such efforts would be unfortunate. Risk-based cybersecurity practices, in which defined resources are allocated against perceived threats according to the anticipated level of risk, inevitably require hard decisions and judgment calls. Allowing the plaintiffs’ bar to string together a few of these hard decisions into a narrative drawn with the benefit of hindsight is neither fair nor productive. Companies should be encouraged to explore their risks and make business judgments in response—these discussions and judgments should not be chilled by the threat of second guessing through litigation.

~~~~~

If courts permit the use of enforcement actions and class action litigation to generate data-security standards on a post hoc basis, that approach would run the risk of imposing potentially massive liability on companies. At the same time, it would threaten to turn companies’ focus away from appropriate cybersecurity practices based on risk and instead towards wooden compliance with a checklist of practices that may reduce future liability risk, but do not advance enterprise security. As the Wyndham case and the Heartbleed bug illustrate, the blunt instruments of FTC enforcement actions and class action litigation are likely to generate only waste and confusion in the arena of cybersecurity. Courts, policymakers, and the public should demand better.
In LabMD, Inc. (“Lab”) v. Federal Trade Commission ("FTC"), C.A. No. 1:14-cv-00810, (N.D. Ga. May 12, 2014) the court held that it did not have jurisdiction to decide the plaintiff’s challenge to an FTC enforcement action regarding the fairness of the plaintiff’s cybersecurity practice because the agency’s actions were not final and because the Leedom exception to the exhaustion rule did not apply. In so ruling the court rejected plaintiff’s arguments that the FTC does not have jurisdiction under Section 5 of the FTC Act to address data security issues in the health care field that are already being regulated by the Department of Health and Human Services, and that the FTC has not provided constitutionally sufficient warning of what it requires. The case is important because it will set a precedent for judicial review of future FTC enforcement orders.

The FTC brought an administrative action against Lab, charging it with violating Section 5 of the FTC Act, which generally empowers the FTC to prevent persons from using unfair acts or practices in or affecting commerce. The FTC charged Lab with failing to protect consumers from disclosure of their sensitive personal information.

According to the FTC, the impetus for the investigation into Lab originated in 2009 when the FTC learned that sensitive personal information in Lab’s possession had been made available to the public on a peer-to-peer file sharing network. In early 2010, the FTC undertook an investigation into Lab’s data security practices. The investigation culminated with the FTC’s filing of an administrative complaint against Lab on 8-28-13. The FTC charges Lab under Section 5 with failure to provide reasonable and appropriate data security for personal information on Lab’s computer networks. The FTC also alleges that Lab could have corrected its problematic practices at relatively low cost using readily available security measures, whereas consumers harmed by Lab’s security failures could not have taken steps to protect themselves.

On 11-12-13, Lab moved to dismiss the complaint on jurisdictional grounds. On 1-16-14, the FTC issued its order denying Lab’s motion to dismiss, holding that the FTC had jurisdiction under Section 5 to address the data security issues and that the FTC had not
violated Lab’s right to due process (the “January Order”). The FTC further determined that the ultimate decision on Lab’s liability would depend on the factual evidence.

The parties proceeded with discovery and an evidentiary hearing was scheduled to begin on May 20, 2014. Lab brought an action in District Court of Georgia seeking an injunction against the continuation of the proceeding and a declaration that the FTC exceeded its authority, violated Lab’s due process rights, and unconstitutionally retaliated against Lab for protected First Amendment speech. Lab asserts five grounds for relief: (1) violation of Administrative Procedure Act (APA) in that FTC’s actions were arbitrary, capricious, an abuse of discretion and power, and unconstitutional; (2) ultra vires agency action for non-statutory violations; (3) fair notice due process violation; (4) facial and structural due process violation; and (5) retaliation for protected First Amendment speech.

The FTC moved to dismiss on two grounds: (1) the District Court does not have subject matter jurisdiction to block an ongoing administrative proceeding; and (2) Lab fails to state a claim that challenges the FTC’s authority to address data security practices. Following is a summary of the arguments made in the briefs. Many of the arguments are related and intertwined.

Subject Matter Jurisdiction

The essence of the FTC’s argument is that its January Order determining that it has authority under Section 5 to address data security issues in the health care field is not “final agency action.” Since it is not final, it is not reviewable by the federal courts, citing the Supreme Court decisions in Thunder Basin Coal Co. v. Reich, 500 U.S. 200 (1994), Ewing v. Mytinger & Casselberry, Inc., 339 U.S. 594 (1950), and FTC v. Standard Oil, 449 U.S. 232 (1980) and their progeny.

More specifically, the FTC argues that under the Supreme Court decision in Thunder Basin, district courts lack jurisdiction to consider any claims related to an ongoing administrative proceeding when Congress intended to foreclose interlocutory review. The FTC claims that is the case here. It notes that under the FTC Act, Congress vested the court of appeals with exclusive jurisdiction to review any final agency cease-and-desist orders. Such grant of exclusive jurisdiction demonstrates that Congress intended to preclude challenges prior to completion of the agency proceedings. If a district court could review interlocutory orders, this would be inconsistent with Congress’ grant of exclusive jurisdiction for review of final agency action to the court of appeals.
Similarly, with respect to injunctive relief in particular, the FTC argues that *Ewing* and its progeny establish that enjoining ongoing administrative proceedings is not available from any federal court. An injunction would be unnecessary and premature judicial interference.

The FTC states that *Standard Oil* held squarely that the FTC’s issuance of an administrative complaint is not final agency action subject to judicial review. It further argues that under *Standard Oil*, FTC’s denial of a motion to dismiss is also not final agency action, even when the denial rejects an argument that the FTC exceeded its authority. The FTC takes the position that the January Order, though a definitive ruling that Section 5 applies to data security, does not render the administrative proceeding final under the APA.

Alternatively, the FTC argues that application of the factors discussed in *TVA v. Whitman*, 336 F.3d 1236 (11th Cir. 1990) demonstrates that the Court should not exercise subject matter jurisdiction, to wit: (1) the January Order does not affect Lab’s legal rights and obligations because it does not resolve whether Lab’s practices are unreasonable or require any action on Lab’s part; (2) there is no immediate impact on Lab’s daily operations, again because the January Order does not require any action by Lab; (3) the district court action does not involve pure questions of law because there are substantial facts to be resolved at the administrative evidentiary hearing; and (4) judicial review at this point would be inefficient because it would prevent the FTC from examining Lab’s conduct.

As a related but similar argument, the FTC argues that Rule 12(b) requires dismissal of unripe claims, and that Lab’s claims are unripe because they depend upon the occurrence of far from certain contingencies. At this point, whether Lab’s data security practices were unreasonable is a fact question to be resolved in the administrative proceeding and it is impossible to know how FTC will resolve the matter. The FTC acknowledges that Lab takes the position that the FTC ultimately votes in favor of Commission counsel in every case and therefore the outcome is “predetermined.” To dispute that contention, the FTC makes note of its recent opinion that reverses an Administrative Law Judge’s rulings holding the respondent liable.

**FTC Authority**

The Complaint avers that the FTC lacks authority to regulate data security because Section 5 of the FTC Act says nothing about data security. It also avers that Congress divested any possible FTC authority over data security in the health field when it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) which are administered by the Department of Health and Human Services (HHS).
The FTC argues that HIPAA and HITECH do not divest the FTC of Section 5 authority. It asserts that multiple statutes can coexist absent a clearly expressed congressional intent to the contrary, and that neither HIPAA nor HITECH forecloses the possibility that another agency plays a parallel role in protecting patient data security. In addition to case authority, the FTC cites statements made by HHA that HIPAA regulations establish a minimum level of security, and that covered entities can be required by other federal law to adhere to more stringent security measures. The FTC also cites the District Court of New Jersey’s decision in *FTC v. Wyndham Worldwide Corp.*, Civil Action No. 13-1887(ES) (D. N.J. April 7, 2014), issued that very day, holding that the FTC Act confers on the FTC authority over data security practices and that other statutes that also address data security do not impliedly preempt the FTC Act.

The FTC argues that in the absence of any basis for believing that HIPAA and HITECH displace FTC authority, the FTC’s interpretation of the scope of its jurisdiction under Section 5 as set forth in the January Order is reasonable and is entitled to *Chevron* deference\(^1\). It cites the Supreme Court’s statement in *City of Arlington v. FCC*, 133 S.Ct. 1863 (2013) that an agency’s interpretation of its statutory jurisdiction is no different from its interpretation of any other part of the statute it administers, and is entitled to the same deference.

The FTC further argues that it does not matter that Section 5 does not itself mention data security. Section 5 broadly empowers the FTC to take action against any unfair act or practice in commerce that could cause substantial injury to consumers and which is not reasonably avoidable by the consumers themselves. Section 5 therefore does not delineate all specific kinds of practices, but allows the FTC to define unfair practices on a flexible, incremental basis, to keep pace with ever-changing methods of consumer harm. The FTC cites a string of cases, including *Wyndham*, holding that Congress did not intend to confine the forbidden practices to fixed and unyielding categories.

**Ultra Vires**

Lab avers in its Complaint that the FTC violated various statutes, and that such *ultra vires* conduct provides a basis for subject matter jurisdiction. The FTC argues that none of those statutes were violated or are relevant here.

\(^1\) Although not explained in the FTC’s brief, it is noted here that *Chevron v. NRDC*, 467 U.S. 837 (1984) sets forth rules for judicial review of an agency’s statutory interpretation. It provides that where a statute is ambiguous, if the agency’s determination is based on a permissible construction of the statute, the court should defer.
First, the FTC contends that 15 U.S.C. §45(m)(1)(B)—which addresses when the FTC may commence an action to obtain a civil penalty—is irrelevant because the FTC has not sued Lab in federal court and is not currently seeking a civil penalty.

Second, the FTC asserts that it is not in violation of 5 U.S.C. §552(a)(1)—which requires agencies to publish the results of formal notice and comment rulemaking—because the FTC has not adopted any rules subject to that provision.

Third and finally, the FTC argues that it has not violated 15 U.S.C. §45(n)’s prohibition against using public policy as its prime motivation in bringing an enforcement action against Lab. The FTC asserts that Lab’s contention that the FTC has violated the statute is a conclusory and naked assertion.

**Fair Notice Due Process**

The FTC argues that Lab does not demonstrate a fair notice due process violation because (a) no liberty or property interest of Lab has been implicated; (b) due process does not require the FTC to issue data security regulations before bringing an enforcement action against Lab; and (c) the FTC is not using an unconstitutionally vague standard.

The FTC asserts that Lab does not demonstrate that its liberty or property interest is implicated because Lab’s assertion of injury is too remote and speculative. No cease and desist order has been entered yet, and Lab is not being required to do anything or pay any penalty.

With respect to the need to issue regulations, the FTC asserts that the courts have rejected a rigid requirement for promulgating regulations, and have approved the FTC’s case by case approach. The FTC relies on a string of decisions from the Supreme Court and other courts, including the *Wyndham* decision, finding that the FTC has discretion to decide whether to address an issue by rulemaking or by case by case adjudication. Factors may vary from case to case, rigid rules may not be helpful, or a problem may be so specialized and varying in nature as to be impossible to capture within general rules.

Similarly, the FTC contends that its determination that Section 5’s general prohibition against unfair practices includes the failure to maintain reasonable data security measures does not establish an unconstitutionally vague behavioral standard. The FTC relies primarily on *SEC v. Chenery*, 332 U.S. 194 (1947), *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374 (1965), and *Am. Gas Ass’n v. FERC*, 912 F.2d 1496 (D.C. Cir. 1990) for the proposition that agencies may use broad terms to describe impermissible conduct without running afoul of the void-for-vagueness doctrine. Specific regulations cannot begin to cover the infinite variety of conditions which companies face regarding data security.
**Due Process**

The FTC argues that Lab does not demonstrate any “facial and structural due process violations” because (a) the FTC’s structure and rules of practice do not violate due process; and (b) there is no *ex post facto* claim.

Lab asserts in its Complaint that it violates due process for the FTC to determine a motion to dismiss its own administrative proceeding, *i.e.* to be both prosecutor and judge. The FTC cites various authorities for the proposition that courts have long ago rejected the idea that combining judging and investigative functions is a denial of due process. The FTC also points out that the APA and the FTC Act authorize the FTC to review an administrative law judge’s determinations *de novo*. It therefore cannot violate due process for the FTC to make the determination in the first place.

In addition, the FTC argues that Lab’s claim that the FTC has violated the prohibition on *ex post facto* law enforcement must be dismissed because the prohibition applies only to laws that are criminal or penal in nature, which this is not.

**First Amendment Retaliation**

The Complaint avers that the FTC’s enforcement action against Lab was in retaliation for the public comments of Lab’s president critical of the FTC. The FTC contends that Lab’s claim for First Amendment retaliation fails to meet the standard set by the Supreme Court in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007)—that in order to survive a 12(b)(6) motion to dismiss, a complaint must state a “plausible” claim for relief.

The FTC contends that Lab fails to meet this test because the allegations of the Complaint do not plausibly infer a nexus between the president’s criticism of the FTC in his book and other public statements and the FTC’s action against Lab. The FTC asserts that the president’s criticism did not begin until after the investigation started in 2010 and his book was not published until 2013. The FTC also argues that the standard for showing improper selective enforcement is demanding and agency officials are entitled to a presumption that they properly discharged their official duties.

**Motion for Preliminary Injunction**

The FTC argues that Lab’s motion for a preliminary injunction must be denied because Lab fails to satisfy the four factors required for preliminary injunctive relief. First, Lab fails to demonstrate likelihood of success on the merits because the court lacks subject matter jurisdiction and Lab fails to state any claim upon which relief can be granted. The FTC asserts that this is the most important factor.
Second, Lab fails to show the possibility of irreparable injury because any litigation expense that Lab will experience by awaiting the FTC’s final determination is not considered irreparable injury. Moreover, Lab has not explained how the alleged imminent lapse of its insurance policy creates an irreparable injury or exigent circumstances. In addition, Lab will not suffer any harm to its First Amendment rights since its president is free to continue to engage in speech critical of the FTC.

Treating the third and fourth factors together, the FTC argues that the balancing of the equities and consideration of the public interest tips in its favor. The FTC asserts that it, and the public, each have a strong interest in an orderly administrative process, unencumbered by premature involvement by the federal courts.

Lab’s Response

At the beginning of its brief, Lab summarizes its main arguments as follows:

(1) The FTC issued the January Order taking for itself the power to add its own arbitrary and idiosyncratic requirement to HHS’s HIPAA regulations for data security. Because the January Order is the FTC’s final word on its jurisdiction under Section 5, but is not a cease and desist order reviewable by the court of appeals, it is reviewable now in the district court.

(2) There is no support for the FTC’s blanket claim that Article III courts are always prohibited from interfering with ongoing administrative proceedings.

(3) Application of the FTC’s own four factor test from TVA v. Whitman for whether subject matter jurisdiction should be exercised demonstrates that judicial review is proper now.

(4) Lab is suffering immediate irreparable harm. The FTC’s enforcement actions beginning in 2010 have cast a shadow over Lab’s operations, and because the FTC never told Lab what it did wrong until it provided Lab with an expert report in March 2014, the FTC prevented Lab from curing any flaws, assuring its customers and preserving its business.

(5) None of the FTC’s arguments prohibits the district court from protecting Lab’s constitutional rights or allows the FTC to put a company out of business without alleging specific regulatory violations.

Each argument is discussed in greater detail below. Lab intertwines the arguments among its discussion of the issues of subject matter jurisdiction, sufficiency of the Complaint and the need for preliminary injunctive relief, since each affects the others. Its brief is not a point by point response to the FTC’s Brief.
Lab argues that the January Order was a final determination by the FTC with respect to its jurisdiction to regulate data security practices under Section 5 of the FTA Act. No further legal action is required with respect to that legal issue.

Lab points out that the FTC admits in its brief that the January Order is “a determinative interpretation of the application of Section 5.” Lab also notes that the FTC considered the January Order to be final enough to submit it to the Eleventh Circuit and the District Court in New Jersey in the Wyndham case, and to ask those courts to apply Chevron deference to the Order. Lab asserts that only final agency actions construing a statute are entitled to Chevron deference. It also relies on Loving v. IRS, 742 F.3d 1013, 1022 (D.C. Cir. 2014) for the proposition that the “fox-in-the-henhouse syndrome” of an agency determining its own jurisdiction is to be avoided “by taking seriously, and applying rigorously, in all case, statutory limits on agencies’ authority.”

Thus, Lab argues that since the FTC has treated the January Order as final agency action, it is now reviewable, citing the Supreme Court decision in Sackett v. EPA, 132 S.Ct. 1367 (2012). Since the Eleventh Circuit does not have jurisdiction until a final cease and desist order is entered, all other final agency actions are reviewable in district court under 28 U.S.C §1331 and 5 U.S.C. §702.

Lab attempts to distinguish the cases relied upon by the FTC. It argues that Standard Oil and its progeny do not apply because Lab is not challenging the issuance of the administrative complaint. Rather it is challenging final agency action in the form of the January Order.

It argues that Ewing does not apply because the January Order is not the type of preliminary decision addressed in Ewing. More important, the dissenting opinion of Justice Frankfurter in Ewing identifies the concerns that are squarely presented in this case and warrant immediate judicial review—i.e. the question of “whether [the Act] has been so misused by refusal of administrative hearing, together with irreparable injury in anticipation of judicial hearing, as to deny appellee due process of law or to amount to an abuse of process of the courts.”

Lab characterizes Thunder Basin as a decision which “solely addressed limitations on jurisdiction to review purely statutory claims before the agency initiated an enforcement action.” Lab contends that the only constitutional issue was the timing of the suit and the Court reached the merits of that claim. Here, Lab is challenging on ongoing enforcement proceeding on constitutional and jurisdictional grounds. Also the statute involved in
Thunder Basin expressly provided that “no objection that has not been urged before the Commission shall be considered” by the court of appeals. This does not bar review here.

Similarly, Lab contends that the ripeness doctrine does not preclude judicial review in this case. The January Order is a final and determinative statement of the FTC’s authority to act in this matter, Lab disputes the FTC’s scope of authority, and Lab has suffered and continues to suffer injury. Thus the matter is ripe for adjudication.

**District Court Jurisdiction**

Lab further argues that even if the January Order is not considered final agency action, the District Court still has jurisdiction to redress FTC abuses and irreparable harm prior to the issuance of a cease and desist order (at which point the court of appeals has exclusive jurisdiction). Lab cites, among other examples, the decision in *E.I. du Pont de Nemours & Co. v. FTC*, 488 F.Supp. 747 (D. Del. 1980), in which DuPont did not exhaust its administrative remedies but filed a declaratory judgment action. The court concluded it had subject matter jurisdiction to hear the claim, explaining that the FTC Act does not deprive district courts of jurisdiction to review orders action taken during the course of an administrative proceeding when a cease and desist order has not yet issued.

As a separate but similar argument, Lab asserts that district courts have subject matter jurisdiction to redress agency actions that are demonstrably *ultra vires* or unconstitutional, even where a statute requires some agency decisions to be reviewed directly in the court of appeals, citing among other things the Supreme Court decision in *Sackett*. Lab avers in its Complaint and its brief that the following FTC actions were *ultra vires*: (a) FTC violated 15 U.S.C. §45(m)(1)(B)’s prohibition against using consent orders against third parties to create a “common law” of data security; (b) FTC violated 5 U.S.C. §552(a)(1) by failing to publish standards and requirements in the Federal Register; and (c) FTC violated 15 U.S.C. §45(n)’s prohibition against using unilateral unstated public policy considerations as a primary basis for exercising its “unfairness” authority. Lab disputes FTC’s claim in its main brief that these statutes are irrelevant here.

Lab also argues that the District Court has subject matter jurisdiction over its First Amendment retaliation claim. Lab’s president published a book criticizing FTC, which is protected speech. Thereafter, the FTC filed its administrative complaint. Such reprisal violates the First Amendment. Thus, Lab states a claim for First Amendment retaliation. In essence, Lab asserts that since it states claims for *ultra vires* and constitutional abuse, the District Court has subject matter jurisdiction to hear those claims.
In response to the FTC’s argument that consideration of the factors discussed in *TVA v. Whitman* requires dismissal, Lab contends just the opposite—that application of those same factors supports subject matter jurisdiction, *i.e.*:

1. Lab’s legal rights and obligations are affected because the January Order determines that the FTC may add by “common law” new data security obligations on top of HHS’s obligations and that Lab must comply with them;

2. The FTC proceeding has and will have an immediate impact on the daily operations of the regulated party because the FTC investigation has “driven the company into the ground.” Lab asserts that as a result of the four years of investigation and administrative proceedings, Lab has had to lay off almost all of its employees and has been forced to curtail the services it offers. Lab claims that the FTC has “crippled” Lab because of the FTC’s failure to specify what it considers to be impermissible practices in the data security area;

3. Pure questions of law are involved in that the core issue in this action is a legal question concerning whether the FTC may lawfully over-regulate HIPAA regulations and if so, whether the FTC has provided fair notice; and

4. Pre-enforcement review will be efficient because if the FTC lacks jurisdiction to over-regulate, then the grinding administrative proceeding must end. There is no efficiency for doctors, hospitals and medical laboratories, or the general public, if the FTC abuses its power.

**Preliminary Injunction**

Lab asserts irreparable harm based on injury to its business, loss of customers, and loss of good will that has incurred and continues to be incurred. Among other things, it claims that its CGL insurer will not renew its policy in May 2014 due to the FTC, and this will force it out of business. It claims that its physician clients have lost confidence in the company due to its inability to explain, and the lack of opportunity to cure, whatever the FTC considers to be “wrong” with its data security practices. It states that it had to lay off almost all of its employees. Lab claims to be literally “fighting for its survival” due to the FTC’s decision to over-regulate the HIPAA regulations. Lab cites case law stating that the type of harm affecting Lab is irreparable. It cannot recover money damages against the FTC due to sovereign immunity.

Lab identifies the core question at issue in this action as “the breadth of FTC’s Section 5 unfairness authority.” Lab asserts that Congress never intended the FTC to have such sweeping and over-riding authority to intervene and impose new and additional requirements on
entities that are already regulated by sister agencies. Lab asserts that an injunction is required to stop the FTC from swallowing the HIPAA data security program and any other regulatory regime that is not to FTC’s liking.

Lab argues that this action is controlled by the Supreme Court decision in *Credit Suisse Securities (USA) LLC v. Billings*, 551 U.S. 265 (2007), in which the Court set forth a four factor test for determining when a specific regulatory regime displaces or implicitly precludes enforcement under a more general and earlier enacted statute. Applying those factors shows that HIPAA regulation of data security is incompatible with FTC over-regulation:

1. HIPAA directly applies and delegates rulemaking authority to HHS;
2. HHS has in fact adopted data privacy and security rules, which it enforces;
3. Dual enforcement by the FTC and HHS is resulting in and will continue to result in conflicting guidance and requirements. As an example, Lab offers a Declaration from a consultant on HIPAA who says that the FTC expert report requires Lab to use some form of encryption, whereas encryption was considered, but rejected in the HIPAA regulations; and
4. Data security is an area that HIPAA specifically addresses through express statutory authority and HHS has adopted requirements based on a balancing of interests that differ in material ways from the FTC’s program, which does not consider those same interests. As an example, Lab notes that HHS is required by HIPAA to address the needs and capabilities of small health care providers and that HHS emphasizes that its rules must be “scalable” so that they can be effectively implemented by covered entities of all types and sizes. The FTC ignores scalability as a pertinent factor in a data security program.

As discussed above, the FTC relies on Judge Salas’s recent decision in *Wyndham* holding that the FTC Act confers on the FTC authority over data security practices, and that other statutes that address data security do not impliedly preempt the FTC Act in this area. Lab attempts to distinguish the *Wyndham* decision on the ground that Wyndham was not already regulated by another statute, whereas Lab is already regulated by HIPAA. Thus, Judge Salas did not address the issue of over-regulation that is at issue here. He did not imply that the FTC may over-regulate HIPAA providers and engage in “common law” enforcement without disclosing to the providers what additional security data requirements applied. Lab further argues that even if *Wyndham* is controlling, it was wrongly decided under controlling Supreme Court and Eleventh Circuit precedent.
In response to the FTC’s claim that Lab does not state a due process claim because it cannot show that its liberty or property interests are being implicated, Lab points out that it is not just talking about litigation expense. If the FTC finds against Lab, Lab will be compelled to act and be subject to an array of burdensome financial requirements. Lab rejects the FTC’s assertion that this chain of events is too attenuated. It avers that no respondent has prevailed in an FTC administrative case in nearly 20 years, so it is a statistical certainty that FTC will rule against it. Lab contends that the one example the FTC cites to show that it can rule in favor of a respondent in fact still resulted in a liability finding.

In response to the FTC’s argument that Section 5 is not unconstitutionally vague, Lab points out that Section 5 is merely a general prohibition of unfair trade practices. It does not expressly mention data security or specify standards. Thus, the statute itself does not provide constitutionally adequate notice of what the FTC considers permissible or impermissible. Lab argues that the cases relied upon by FTC are not controlling. For example, *Chenery* is not a fair notice case and the SEC did not seek to impose liability for past conduct as FTC is doing here. Similarly, *Am. Gas Ass’n* did not involve an agency attempting to impose future liability for past conduct. *Colgate-Palmolive* was not an “unfairness” case but a “deception” case raising different concerns.

Lab asserts that the only harm faced by the FTC is being prevented from enforcing its laws. This is true every time government action is challenged. It is far outweighed by the economic harm to Lab. Similarly, public interest favors injunctive relief here. Lab contends that the public does not want unconstitutional and unauthorized enforcement actions. Further, pre-enforcement review of the legal questions in this case will assist the FTC in determining the scope of its authority, thus ensuring that the final relief is within that authority.

**FTC Reply Brief**

In addition to reiterating arguments made in its main brief, the FTC made some specific responses to arguments made by Lab, as follows.

The FTC asserts that Lab is wrong that *Thunder Basin* applies only to review of purely statutory claims before the agency instituted enforcement action and that the court reached the merits of the case. The FTC contends that in *Elgin v. Dept. of Treasury*, 132 S.Ct. 2126 (2012), the Supreme Court rejected that very reading of *Thunder Basin*.

The FTC says that Lab’s reliance on the dissenting opinion in *Ewing* is unavailing in light of the unbroken line of authority from Ewing that courts may not interfere with the administrative process even in the face of constitutional and jurisdictional challenges.
The FTC cites two new cases on the ripeness doctrine, but its argument remains the same—that any review of the FTC’s jurisdiction ruling is not ripe until a final cease-and-desist order is issued and can be reviewed by the court of appeals.

With respect to Lab’s claims of hardship and irreparable injury, the FTC asserts that “casting a shadow” over a litigant’s business is not enough to justify immediate judicial intervention.

The FTC reiterated that *Standard Oil* holds that an administrative complaint is not final agency action, even though it is definitive on the question of whether the FTC had reason to believe that the respondent violated the FTC Act. For the same reason, *Standard Oil* requires that the January Order not be considered final agency action, even though it is definitive on the question of whether the FTC has jurisdiction to regulate data security under Section 5.

The FTC says that Lab’s attempt to invoke the narrow doctrine of “non-statutory” review where a court can rein in an agency that is acting *ultra vires*, is unavailing. Lab’s *ultra vires* claims do not fit into the narrow exception established in *Leedom v. Kyne*, 358 U.S. 184 (1958). That exception is limited to cases where (1) the agency acted outside the scope of its designated powers and contrary to “clear and mandatory” statutory provisions; and (2) the litigant would be wholly deprived of a meaningful and adequate means of vindicating its rights. The FTC claims that Lab does not satisfy either element.

The FTC disputes Lab’s reliance on *Loving* in support of its argument that the January Order is not entitled to *Chevron* deference. The FTC argues that in *Loving*, the statute itself indicated that the agency did not have jurisdiction and the agency’s interpretation of the statute was unreasonable. Here, Section 5 is worded broadly and the FTC has consistently asserted authority over data practices.

With respect to Lab’s argument that HIPAA divests the FTC of authority to regulate data security, the FTC asserts that Lab does not show any incompatibility between FTC authority and HIPAA, and does not give any example of conflict between the dual enforcement regimes. (Lab in fact did give such examples in its brief, but the FTC fails to address those examples.) The FTC asserts that Lab’s reliance on *Credit Suisse* is misplaced because it did not alter decades of established preemption law requiring that the two laws be “clearly incompatible.”

The FTC takes issues with Lab’s attempt to distinguish *Chenery* on the ground that in this case, the FTC is seeking to impose future liability for past conduct. To the contrary, the FTC notes that it can require Lab to cease and desist going forward, but it may not impose any monetary damages for past behavior.
Finally, the FTC reiterates that Lab’s First Amendment retaliation claim does not pass the *Twombly* plausibility test. Lab’s allegation that its president published a book and then the FTC filed its administrative complaint does not establish a sufficient causal connection. The FTC’s investigation had been underway for three years before the book was published, so the FTC could not have been motivated to retaliate for the book.

**Relation to *FTC v. Wyndham***

As discussed above, the briefs relate to the *Wyndham* case in several ways.

The FTC relies on the *Wyndham* decision as support for the following propositions:

(1) The FTC Act confers on the FTC authority over data security practices, and other statutes that address data security do not impliedly preempt the FTC Act in this area;

(2) It does not matter that Section 5 does not itself mention data security. Section 5 is intentionally broad and allows the FTC to define unfair practices on a flexible, incremental basis, to keep pace with ever-changing methods of consumer harm; and

(3) Due process does not require the FTC to issue data security regulations before bringing any enforcement action. The agency has discretion to decide whether to address an issue by rulemaking or by case-by-case adjudication. The problem can be so specialized and varying in nature as to be difficult to capture within rigid rules, and the agency must retain the power to deal with the issue on a case-by-case basis if it deems that appropriate.

Lab in some ways relies on *Wyndham* and in other ways attempts to distinguish it. On the one hand, Lab notes that the FTC considered the January Order to be “final” enough to submit it to the District Court of New Jersey in the *Wyndham* case and ask the Court to afford the Order *Chevron* deference on the issue of whether the FTC has jurisdiction to regulate data security. That bolstered Lab’s argument that the January Order constitutes final agency action subject to judicial review.

On the other hand, Lab claims that the holdings of *Wyndham* are not controlling in this case. It attempts to distinguish the *Wyndham* decision on the ground that Wyndham was not already regulated by another statute, whereas Lab is already regulated by HIPAA. Thus, Judge Salas did not address the issue of over-regulation that is at issue here. In addition, Lab argues that even if *Wyndham* is controlling, it was wrongly decided under controlling Supreme Court and Eleventh Circuit precedent.
Overview of Recent Data Breach Cases

WIRE ACT; INTERNET; WIRE COMMUNICATION FACILITY; CRIMINAL PROSECUTION


First Circuit Holds That Wire Act Is Applicable to Internet Gambling

COPYRIGHT ACT; DMCA; CFAA; EXTRACTION; SUMMARY JUDGMENT


Sixth Circuit Affirms Grant of Summary Judgment to Defendant in a Suit Regarding the Extraction of Customer Information From Plaintiff’s Database

WIRETAP ACT; RULE 23; CLASS ACTION CERTIFICATION; GMAIL; SCANNING; PREDOMINANCE; CONSENT


Federal Court Denies Certification to Putative Classes of Gmail Users Because Individual Issues of Consent Would Predominate

CONSUMER PROTECTION LAWS; STANDING; CHOICE OF LAW


Plaintiffs Allegedly Defrauded By Dating Website That Misrepresented Confidentiality of Member Information Unable To Establish Standing Under California Unfair Competition and Consumer Remedies Statutes

ECPA; INTERCEPTION OF DATA; STATUTE OF LIMITATIONS


Plaintiffs Allegedly Deceived Into Joining Valueless Discount Membership Programs Adequately Alleged Their Private Data Was “Intercepted” While in Transit Under ECPA but Claims Were Time-Barred
VIDEO PRIVACY PROTECTION ACT; CLASS ACTION


Federal Court Dismisses VPPA Claims Based on Video Viewing Data
Disclosed to Metrics Company but Allows Claims for Disclosures to
Facebook Finding That Users Could Have Been Linked to Facebook Accounts

STANDING; PLEADING; CA UNFAIR COMPETITION LAW

*In re LinkedIn Privacy Lit.*, Case No.: 5:12-CV-03088-EJD (N.D. Ca. Mar. 28, 2014)

Federal Court Finds Plaintiff Has Standing To Bring
Claims Because California’s Unfair Competition Law
Defines “Advertisement” Broadly Enough To Encompass
Alleged Misrepresentations in LinkedIn’s Privacy Policy

CFAA; DAMAGE; LOSS; TRADE SECRETS; EMAIL; MOTION TO DISMISS


Federal Court Holds That the Costs of Investigating Theft
of Trade Secrets By Means of Unauthorized Copying
of Email Was Not a “Loss” Under the CFAA

FOURTH AMENDMENT; WARRANT; EMAIL; ELECTRONIC DATA; SEIZED; SPECIFICITY

*In the Matter of the Search of Information Associated with [redacted] @mac.com that
is Stored at Premises Controlled by Apple, Inc.*, Magistrate Case. No. 14–228 (JMF) (D.
D.C. Mar. 07, 2014)

Federal Court Refuses To Grant Warrant for Materials Associated
With an Apple Email Address and Instructs the Government
To Narrow Its Search Requests

CFAA; LOSS; WITHOUT AUTHORIZATION; UNAUTHORIZED; MOTION TO DISMISS

*Carnegie Strategic Design Engineers, LLC v. Cloherty*, Civil Action No. 13–1112 (W.D.
Penn. Mar. 6, 2014)

Federal Court Holds That Third Circuit Has Not Yet Ruled on the
Scope of CFAA Liability and Adopts a Narrow Construction of
“Without Authorization” Under the CFAA
CFAA; DAMAGE; LOSS; CALIFORNIA UNFAIR COMPETITION LAW; BATTERY LIFE; MOTION TO DISMISS

In re Google Android Consumer Privacy Litigation, No. 11-MD-02264 JSW (N.D. Cal. Mar. 10, 2014)

Federal Court Dismisses CFAA Claim By Google Users Who Alleged Google Collected Their Personal Data Without Permission .........................85

PRIVACY AGREEMENTS; USER AGREEMENTS; STANDING; DAMAGES; STATE NOTIFICATION LAWS

In re Sony Gaming Networks and Customer Data Security Breach Litigation, MDL No. 11md2258 AJB (MDD) (S.D. Cal. Jan 21, 2014)

Sony PlayStation Data Breach Lawsuit Whittled Down but Moves Forward..........88

THEFT OF PERSONAL INFORMATION; STANDING TO SUE

In re Science Applications International, No. 1:12-mx-00347 (D.D.C. May 9, 2014)

District Court Partially Dismisses Data Breach Case Because Plaintiffs Did Not Allege Actual or Impending Misuse or Viewing of Personal Data .........91

PRIVACY/ SECURITY; PUBLICITY/ PRIVACY RIGHTS

In re Google Android Consumer Privacy Litigation, 1-MD-02264 JSW (N.D. Cal. Mar. 10, 2014)

Yunker v. Pandora, No. 11-CV–03113 JSW (N.D. Cal. Mar 10, 2014)

Android and Pandora Privacy Rulings Accept Low Hurdle for Standing ............104

CONTENT REGULATION. SPAM


Yahoo! Scores Significant Win in Email-to-SMS Lawsuit.................................108

MARKETING


Supreme Court Changes False Advertising Law Across the Country ..................110
LICENSING/ CONTRACTS, PUBLICITY/ PRIVACY RIGHTS

Court Rules That Kids Can Be Bound By Facebook’s Member Agreement ..........113

CONTENT REGULATION. DERIVATIVE LIABILITY

Employer Gets Section 230 Immunity For Employee’s Posts ...............................115

CONTENT REGULATION, INTERNET HISTORY, SEARCH ENGINES

Of Course The First Amendment Protects Baidu’s Search Engine,
Even When It Censors Pro-Democracy Results ....................................................116

EVIDENCE/ DISCOVERY, LICENSING/ CONTRACTS

How To Get Your Clickthrough Agreement Enforced In Court .........................118

E-COMMERCE, LICENSING/ CONTRACTS. MARKETING, PRIVACY/ SECURITY

*In re LinkedIn User Privacy Litigation*, 12-CV-03088-EJD (N.D. Cal. Mar. 28, 2014)
Privacy Claims Based on LinkedIn’s Security
Promises SurviveMotion to Dismiss ..........................................................................121

DERIVATIVE LIABILITY, E-COMMERCE, MARKETING, PRIVACY/SECURITY

*Opperman v. Path*, 2014 WL 1973378 (N.D. Cal. May 14, 2014)
Apple May Be Liable For Privacy Violations by Third-Party Developed Apps ......124

STATE PRIVACY LAWS; FIRST AMENDMENT; ANONYMOUS SPEAKERS

*Digital Music News, LLC v. Superior Court of Los Angeles County*,
No. B242700 (Cal. May 14, 2013)
California Court of Appeals Creates New Argument
for Protecting Anonymous Online Speech ..............................................................142
Recent Decisions

Overview of Recent Data Breach Cases

By

David Dana

The cases regarding data protection that have been decided in recent months illustrate a number of trends in the case law. First, the cases show that potential legal concerns in connection with data protection and data breaches can come from a number of sources, including government suits because a company allegedly inadequately protected customer data or sought customer data in a way that could result in “innocent” customers having their personal information compromised; former employees or business partners taking data in order to gain a competitive advantage, and of course, users of a company’s electronic service claiming that their personal data was copied and/or used by the company without their consent.

Second, the cases show that data protection and data breaches implicate the interpretation of a number of federal and state statutes, and that courts will tie their analysis to the specific words of the statutes. Notably, several cases suggest that California state statutes may be so expansive in their wording that they may provide plaintiffs with the best vehicle to try to establish liability and obtain a recovery. Third, plaintiffs who claim their data was copied or used without their permission are likely to be able to establish standing to sue, but they face obstacles in gaining class certification because of individual consent issues and they are more likely to be able to be allowed to seek equitable relief, including restitution, rather than damages. Because these suits mostly have not proceeded to the summary judgment and/or trial stage of litigation, the attention has focused on legal, rather than factual, questions.

The statute that has received the most attention in the context of suits against former employees or business partners for appropriating data is the Consumer Fraud and Abuse Act. How broadly this statute will be interpreted remains a subject of contention and disagreement among the courts in the different Circuits and sometimes even within the same Circuit. The SBS case from the Northern District of Illinois suggest that companies will not be able to use the CFAA to combat data theft unless they suffered losses to addition to simply the costs of investigating the data breach and its effects. *SBS Worldwide, Inc. v. Potts*, No. 13 C 6557 (N.D. Ill., Feb. 7, 2014). The Carnegie case from the Western District of Pennsylvania suggest that employees who take data using an authorized password but for an improper purpose may not be held liable under he CFAA. *Carnegie Strategic Design Engineers, LLC v. Cloherty*, Civil Action No. 13–1112 (W.D. Penn. Mar. 6, 2014)

The two cases involving the federal government underscore its power in the arena of data protection. In one of these cases, the district court in D.C. denied a sweeping gov-
ernment subpoena directed at Apple and its customers allegedly under investigation, and suggested the government must allow an ISP to perform a search as a first matter and also must explain what will happen ultimately to the data it reviews. At the same time, it remains to be seen whether the government will narrow its subpoenas directed at ISPs. In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., Magistrate Case. No. 14–228 (JMF) (D. D.C. Mar. 07, 2014). In the Wyndham litigation, the district court affirmed broad power of the FTC to bring an action for “unfair” practices in the form of inadequate protection of customer data. FTC v. Wyndham Worldwide Corp. et al., Civil Action No. 13–1887(ES) (D. New Jersey, April 7, 2014). A similar result was reached in in LabMD v. FTC, C.A. No. 1:14-cv-00810, (N.D. Ga. May 12, 2014), where the court declined jurisdiction over the Plaintiff’s challenge to FTC regulation of its security practices because administrative remedies had not been exhausted.

The summaries include four cases involve consumer class actions or putative class actions vened in the Northern District of Columbia, which is clearly now the most influential district for this sort of litigation. In all of these cases, the plaintiffs have been able to survive standing challenges, usually on the grounds that they would not have bought the device (such as the play station in the Sony litigation or the smart phone in the Google Android litigation) if they had known that their data privacy would not be protected. In re Sony Gaming Networks and Customer Data Security Breach Litigation, MDL No. 11md2258 AJB (MDD) (S.D. Cal. Jan 21, 2014); In re Google Android Consumer Privacy Litigation, No. 11-MD-02264 JSW (N.D. Cal. Mar. 10, 2014). However, relying on the Supreme Court’s decision in Clapper v. Amnesty International, other courts deny standing to plaintiffs who have not alleged that a data breach resulted in actual misuse or viewing by others, e.g., In Re Science Applications International, No. 1:12-mx-00347 (D.D.C. May 9, 2014).

These cases underscore the importance of California’s consumer-oriented statutes for plaintiffs: the Court allowed the litigation against LinkedIn to proceed based on its view that “advertising” under California’s Unfair Competition Law is a broad term that includes corporate privacy policies made available to customers or prospective customers, In Re LinkedIn User Privacy Lit., Case No.: 5:12-CV-03088-EJD (N.D.Ca., March 28, 2014). And the Court in the Google Android litigation broadly read the same statute to allow claims to proceed on the grounds that Google’s representations regarding privacy and data allegedly were false, even in the absence of a claim of significant per-class-member losses as a result. Indeed, the Court in that case went so far as to rule that restitution might be due class members from Google under the UCL even though they paid no money to Google. In the same spirit, in the Sony litigation, the Court allowed the claims for restitution under the California Database Breach Act, as well as California’s and other states’ consumer protection statutes, to go forward.
The potentially most important case summarized below ostensibly relates to a purely procedural issue—class certification under Rule 23. The Court in the Google Gmail case denied class certification on the grounds that individual issues regarding members’ consent to gmail scanning would predominate over common issues. The Court held that a broad array of materials, from the company/defendant but also in the press and media generally, could be used to establish an individual’s knowledge of scanning and hence implied consent. Because these kinds of consumer claims can only proceed in practice as class claims, the Gmail decision could, if ultimately affirmed, prevent many consumer claims from proceeding at all. *In re Google Gmail Litigation*, Case No.: 13-MD-02430-LHK (N. D. Cal. 3/18/14)

The summaries also suggest that not any claim under California’s can survive a motion to dismiss: in a case against a dating service, Successfulmatch.com, the Northern District of California dismissed two plaintiffs’ claims under the UCL that they were misled into joining the dating service because they could not identify a specific misrepresentation allegedly made by the defendant. *Doe v. Successfulmatch.com*, No. 13-CV-03376-LHK (N.D.Cal. Apr. 16, 2014)

It also bears noting that in the Hulu class action case, another Northern District of California case, the Court relied on a federal statute, the Video Privacy Protection Act, in denying summary judgment to Hulu, on the grounds that Hulu’s coding had in effect forwarded personally identifiable information of customers to Facebook.

And in a District of Connecticut case, the Court allowed claims against operators of valueless discount membership programs to proceed on the grounds that their personal data had been allegedly “intercepted” within the meaning of the Electronic Privacy Protection Act in that plaintiffs’ allegations described a process in which their confidential billing data, entered on the websites of the defendant online retailers, would be stored on an online “token” and transferred to the defendants selling the memberships. *In re Trilegiant Corporation, Inc.*, No. 3:12-CV-00396 (VLB) (D. Conn. Mar. 28, 2014).

* * *

**WIRE ACT; INTERNET; WIRE COMMUNICATION FACILITY; CRIMINAL PROSECUTION**


**First Circuit Holds That Wire Act Is Applicable to Internet Gambling**

Defendants were convicted for violating the Wire Act, a pre-internet federal statute that provides for criminal penalties for gambling involving a “wire communication facility.” Defendants argued that the Wire Act could not have been intended to cover the internet, as
the internet did not exist when the Act was passed. The First Circuit, however, held that the plain meaning of the term “wire communication facility” in the Wire Act encompasses the internet, and statutes often are read to cover technologies that are invented after their passage. The First Circuit thus affirmed the Wire Act convictions.

Background

Todd Lyons and Daniel Eremian worked for Sports Off Shore (SOS), a gambling business based in Antigua. After a wide-ranging investigation by federal and state law enforcement of SOS and its employees and agents, and a lengthy trial, a jury convicted both Lyons and Eremian on two counts under the Wire Act, 18 U.S.C. § 1084, two counts under RICO, 18 U.S.C. §§ 1962(c) and 1962(d), and one count under 18 U.S.C. § 1955 for conducting an illegal gambling business. Lyons was separately convicted on another eighteen counts. In this direct appeal from their convictions and sentences, Lyons and Eremian argued, among other things, that the Wire Act does not apply to the internet. The Wire Act provides that “[w]hoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers . . . shall be fined under this title or imprisoned not more than two years, or both.”

The Internet and the Wire Act

Lyons and Eremian argued that they should have been granted an acquittal as a matter of law on the Wire Act count that was based on the transmission of information over the internet because, they claimed, the internet is not a “wire communication facility.” According to the First Circuit, citing the Wire Act’s definition of a wire communication facility, “[t]he sufficiency challenge fails because the internet” is an “instrumentalit[y] . . . used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission. 18 U.S.C. § 1081.” Indeed, “[a]nyone reading this opinion on the court’s website or the like would readily agree that the internet is used and useful in the transmission of writings.” As the First Circuit elaborated:

Indeed, it is rather remarkable that a definition written before the internet was invented so accurately describes it. When, as here, the text of a statute “provides a clear answer” to a question of statutory construction our “inquiry ends.” United States v. Robinson, 459 F.3d 39, 51 (1st Cir. 2006). The Wire Act’s evident applicability to the internet likewise means that its application to Lyons and Eremian is not, contrary to their claims, an impermissible ex post facto “novel construction of a criminal statute to conduct that . . . the statute . . . has [not] fairly disclosed to be within its scope.” United States v. Lanier, 520 U.S. 259, 266 (1997).
The argument to the contrary, the First Circuit explained, relied on the misapprehensions that the Wire Act cannot be applied to communications over the internet because the Act was enacted in 1961, before the internet was created and, second, that because the internet is in some manner structurally dissimilar to a telephone or telegraph system, the Wire Act cannot apply to it.

On the first point, we regularly apply statutes to technologies that were not in place when the statutes were enacted. See, e.g., Sec. & Exch. Comm’n v. SG Ltd., 265 F.3d 42, 55 (1st Cir.2001) (Securities Act of 1933 and Securities Act of 1934 applied to virtual shares which exist only in online game); United States v. Nichols, 820 F.2d 508, 511 (1st Cir.1987) (theft statute applied to theft of information from computer network).

Regarding the second point, “nothing in the statute suggests that any instrumentality covered by the Wire Act must be structurally similar to a telephone exchange.”

“Nor is it relevant that the internet is not a common carrier,” as Lyons and Eremian argued. “While section 1084(d) does impose certain requirements on common carriers who are informed their facilities are being used for gambling, nothing in section 1084 or section 1081 limits the application of the Wire Act to transmissions made via common carriers.” The First Circuit thus affirmed the Wire Act convictions, as well as all of the other convictions.

* * *

COPYRIGHT ACT; DMCA; CFAA; EXTRACTION; SUMMARY JUDGMENT


Sixth Circuit Affirms Grant of Summary Judgment to Defendant in a Suit Regarding the Extraction of Customer Information From Plaintiff’s Database

In this suit between two competitors in the alarm industry, plaintiff alleged that defendant violated the Copyright Act, the Digital Millennium Copyright Act (DMCA), and the Computer Fraud and Abuse Act when a former customer of the plaintiff became a customer of the defendant. Plaintiff argued that, in extracting the customer’s information from the plaintiff’s database, the defendant violated all of these statutes. The Sixth Circuit affirmed the district court’s grant of summary judgment to the defendant because the plaintiff did not produce evidence supporting its legal theories, whereas the defendant offered evidence suggesting that the extraction of the customer information did not entail any appropriation of defendant’s code.
Background

Plaintiff-appellant Dice Corporation and defendant-appellee Bold Technologies are competitors that provide services and license software to companies in the alarm industry. Dice claimed that Bold committed a host of intellectual property violations when converting one of Dice’s former customers to its systems. This dispute arose out of a customer defection. ESC Central was a Dice customer for a decade. In 2011, it transitioned to Bold.

Switching software systems is no easy task. The conversion process must be undertaken carefully because the alarm company continues to monitor alarm signals from its subscribers. The transition must be seamless to ensure that the new software is interpreting the incoming alarm signal in the same manner as the old so that no alarm signals are misread or missed.

As part of this transition, Bold extracted ESC Central customer data from Dice’s software databases. Dice maintained that Bold used and copied Dice’s proprietary software in operating the Extraction Program. The district court rejected Dice’s claims in a forty-page opinion, finding them conclusory and devoid of factual support. Dice moved for reconsideration on two grounds. As the district court noted in its opinion denying the motion for reconsideration, “Clifford Dice did not explain how this evidence demonstrated that Bold used Dice’s source code.”

The Copyright Act Claim

Dice alleged that to undertake the extraction process, Bold created an unauthorized derivative work in violation of the Copyright Act, 17 U.S.C. § 106(2). However, Dice did not attempt to demonstrate which aspects of its programs were protectable. Dice did not identify any original elements in its software and did not argue that the receiver drivers represent non-functional expression. Dice failed to identify the original and non-functional elements of its work. “Instead, it provided hundreds of pages of incomprehensible computer code” without explanation other than Clifford Dice’s claim that “Bold’s extraction program utilized Dice source code in the conversion process.”

The DMCA Claim

Dice asserted on appeal that Bold violated the DMCA, 17 U.S.C. § 1201(a), because customers allowed Bold to use their passwords to login to the Dice servers through the “Go To Assist function.” The Sixth Circuit disagreed for two reasons. First, Dice did not cite any evidence of circumvention of technological measures to the district court. “[T]o the extent we are inclined to allow Dice to resurrect its argument, Dice cited no evidence.” Second, Dice’s general theory before the district court was that Bold circumvented Dice’s attempts to encrypt its software. “Dice now argues that Bold violated the DMCA because
ESC Central improperly allowed Bold to use its passwords to login to the Dice software operating at the customer’s site through the Go To Assist function.” “This is a new argument not appropriately considered on appeal.”

The CFAA Claim

Dice argued that the district court erred in dismissing its private cause of action under the CFAA, 18 U.S.C. 1030(g). “Generally, the CFAA protects against unauthorized computer access.” Dice put forward a complex claim of unauthorized access. It claimed that, although ESC Central’s servers running Dice software were owned by ESC Central, they were connected to the Dice disaster recovery network at Dice’s office in Michigan. According to Dice, customer-owned servers, like the ESC Central server running the Dice software, were actually a branch of Dice’s network. “This is because, when a Dice system is installed, Dice’s Michigan servers mirror its customers’ servers.” Thus, according to Dice, when Bold employees accessed ESC Central servers, they necessarily accessed the Dice disaster recovery network. However, even assuming this claim were fairly raised, it would lack merit, as the Sixth Circuit explained:

Liability under the CFAA requires a showing of intentional access. 18 U.S.C. § 1030(a)(2). Neither Narowski nor Condon was aware that performing a Go To Assist Function on ESC Central servers allowed access to Dice servers in Bay City, Michigan. Dice also does not explain how, even if the Go To Assist function allowed access to Dice servers, Condon or Narowski used the Go To Assist function to obtain Dice source code. See 18 U.S.C. § 1030(e)(6). . . . And Narowski attested: “With GoToAssist I cannot access any Dice source code even if the Dice software is running on the customer’s computer which grants access and I have never used GoToAssist to access any Dice source code.” As for Dice’s claim that Condon accessed Dice’s servers to acquire the ALSCHART file, Dice has not presented any evidence.

The Sixth Circuit thus affirmed the district court’s grant of Bold’s motion for summary judgment.

*   *   *
Federal Court Denies Certification to Putative Classes of Gmail Users Because Individual Issues of Consent Would Predominate

In these consolidated cases, class certification was sought for a number of classes and subclasses of gmail users who allegedly had their email scanned by Google without their consent in violation of the federal Wiretap Act and state statutes. The Court denied certification with prejudice, reasoning that individual issues predominated over the common issues. In particular, the Court focused on the issue of whether class members had impliedly consented to having their email scanned, and concluded that this issue required individualized determinations, as there were a wide range of sources from which any individual gmail user might have learned of Google’s scanning practices. The Court held that implied consent need not be based on disclosures by Google itself to gmail users, but could be based on any source of information or report regarding Google’s email scanning.

Background

Plaintiffs alleged that Google violated state and federal antiwiretapping laws in its operation of Gmail, an email service. Plaintiffs challenged Google’s operation of Gmail under state and federal anti-wiretapping laws. “The instant litigation concerns two sets of Google Apps end users.” The first set is comprised of end users of Cable One, an internet service provider that contracts with Google to provide Google Apps-related services to its customers. “The second set of Google Apps end users in this litigation are Google Apps for Education users.” Like Cable One, educational institutions that provided Google Apps services agreed, in their contracts with Google, to obtain the necessary authorization from end users to enable Google to provide the services. The contracts further required Google to comply with Google’s Privacy Policies. Plaintiffs moved to certify four Classes and three Subclasses as Rule 23(b)(3) damages classes. Google did not challenge plaintiffs’ position that the putative Classes meet the numerosity and commonality requirements. Instead, Google contended that none of the Classes satisfies the ascertainability, predominance, and superiority requirements. The Court addressed only the issue of predominance.

Common Issues Do Not Predominate

The Court explained that “[t]he question of whether Class members have consented to the alleged interceptions has been central to this case since its inception.” Specifically,
the issue of whether email users consented to the alleged interceptions was at issue in all rounds of briefing on motions to dismiss, all three rounds of briefing on class certification, and the briefing on the motion for leave to amend.

Courts have interpreted the consent exemption to encompass two different forms of consent. First, consent can be express. Second, in the alternative, consent can be implied in fact based on whether the surrounding circumstances demonstrate that the party whose communications were intercepted knew of such interceptions. Regardless, consent must be actual, and not constructive. *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir.2003) (“Consent may be explicit or implied, but it must be actual consent rather than constructive consent.”).

Importantly, under the Wiretap Act, the statute pursuant to which the Cable One Class, Education Class, Minor Class, and Non–Gmail Wiretap Act Class bring claims, only one party to the intercepted communication needs to consent to render the interception lawful. 18 U.S.C. § 2511(2)(d).

The Court found that with respect to the Education Class, the substantial individual questions regarding the nature of each Google Apps Administrator’s disclosures are likely to lead to individual questions regarding express consent that will predominate over common questions.

The Court need not determine whether class-wide express consent questions will predominate over individual questions with respect to the Minor Class, Cable One Class, and the Non–Gmail User Classes because . . . the Court finds that individualized questions regarding implied consent will overwhelm any common issues regarding these Classes.

“Implied consent is an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted.” The Court found that individual issues regarding consent are likely to overwhelmingly predominate over common issues. As the Court explained:

Specifically, there is a panoply of sources from which email users could have learned of Google’s interceptions other than Google’s TOS and Privacy Policies. First, Class members could have learned of the interceptions from various Google sources. For example, the “About Ads on Search, Gmail and across the web” page, which has been viewed more than a million times, states that “[t]he ads you see [in Gmail] may be based on many of the same factors as ads in Google Search as well as additional factors like the messages in your mailbox” and provides the following example: “You’ve recently received lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a local camera store.” Chin Decl. ¶¶ 41, 43; id., Ex. DD. Furthermore, the link for “Why This Ad?” next to each targeted advertisement in Gmail, which led users to the disclosure that “[t]his ad is based on emails from your inbox,” was clicked thousands of times in every day. *Id.* ¶ 56; *id.*, Ex. JJ. Second, Class members may
have learned about the alleged interceptions from various media sources. For example, a 2004 Houston Chronicle article states that “some industry watchers have complained that Google scans account holders’ messages for keywords and then delivers text-based ads relevant to the keywords detected. However, most Gmail users said they’re not bothered by it.” . . . Along a similar note, a Washington Post article stated, “Google’s Gmail service has generated some controversy among privacy activists for the way its technology serves up text ads to users based on the content of their messages. None of the Gmail account holders or would-be account holders contacted for this article expressed concerns along these lines.”

As the Court noted, “[s]ome Class members likely viewed some of these Google and non-Google disclosures, but others likely did not.” A fact-finder, in determining whether Class members impliedly consented, would have to evaluate to which of the various sources each individual user had been exposed and whether each individual “knew about and consented to the interception” based on the sources to which she was exposed. “This fact-intensive inquiry will require individual inquiries into the knowledge of individual users,” and “[s]uch inquiries—determining to what disclosures each Class member was privy and determining whether that specific combination of disclosures was sufficient to imply consent—will lead to numerous individualized inquiries that will overwhelm any common questions.” Thus, common issues did not predominate over individual ones.

Plaintiffs contended that in determining whether Gmail users impliedly consented, the finder of fact should be limited to looking at a uniform set of Google’s own disclosures, rather than to disclosures of third parties. Plaintiffs also contended that the parol evidence rule precludes the finder of fact from looking outside the contractual agreements between Gmail users and Google. The Court disagreed.

The Court explained that, even “if Plaintiffs were correct regarding the scope of documents to which a fact-finder could look, there would be a myriad of individual issues with respect to consent, because Google itself had several disclosures, which could not have been uniformly viewed by Class members.” “In light Google’s own disclosures’ diversity, even accepting Plaintiffs’ theory, a fact-finder would have to evaluate whether consent could be implied from the specific set of Google disclosures that each individual user encountered.”

Moreover, the Court saw no basis as to why the disclosures relevant to a fact-finder’s determination of implied consent should be limited exclusively to Google disclosures. As the Court explained:

[C]ourts have held that the question of implied consent turns on whether the party whose communications were intercepted had notice of the interception or consented to the interception based on all of the surrounding circumstances. Berry, 146 F.3d at 1011; Griggs–Ryan, 904 F.2d at 117; Amen, 831 F.2d at
378. Plaintiffs do not cite any authority limiting the sources from which such notice or knowledge can be acquired, nor could this Court find such authority. Accordingly, the Court concludes that the full panoply of disclosures, from the news media, from Google, and from other sources, is relevant to the question of whether consent to the alleged interceptions should be implied from the surrounding circumstances. Plaintiffs contend that relying on extrinsic evidence outside of Google’s agreements with Class members would violate the parol evidence rule or that consideration of such evidence would be prohibited by the merger clause in the TOS. While these could be valid contentions if Plaintiffs stated a breach of contract cause of action, these are not viable arguments with respect to the consent under the Wiretap Act, which requires the fact-finder to consider all the surrounding circumstances to determine whether an individual knew that her communications would be intercepted.

Plaintiffs relied exclusively on a Northern District of Illinois case, *Harris v. comScore, Inc.*, 292 F.R.D. 579, 585 (N.D.Ill. 2013), for their proposition regarding the parol evidence rule. The Court, however, found *Harris* unpersuasive. The *Harris* court held that

ComScore [the intercepting entity] contends that the scope of consent will vary for each plaintiff depending on his subjective understanding of the agreement and the surrounding circumstances. In support, comScore notes that at least under the ECPA, consent need not be explicit, but can also be implied from the surrounding circumstances. But that rule has no place where a party manifested consent through the adoption of a form contract.

For the proposition in the last sentence, however, *Harris* merely cited a Seventh Circuit case interpreting Illinois contract law. The *Harris* court did not address the long line of cases that suggest a broader swath of materials is relevant to implied consent under the Wiretap Act. The Court concluded:

“Furthermore, Plaintiffs’ contention that a finder of fact may only look to the agreements between Google and its users in determining consent improperly collapses express and implied consent.” As the Court explained:

The agreements between Google and its users define the scope of the universe of material that the Court may consider in determining whether Plaintiffs have *expressly consented*. If the fact-finder were limited to the same material for purposes of determining implied consent, then express and implied consent would be coterminous. Courts have recognized, however, that express and implied consent are analytically distinct.

In sum, the Court found that a fact-finder would have to determine to what disclosures each Class member was exposed and whether such disclosures were sufficient to conclude, under the Wiretap Act, that Class members consented to the alleged Google interceptions of email. “This factual inquiry is an intensely individualized one.” Furthermore, the myriad
disclosures among the various Google Apps for Education Administrators raised a variety of individualized questions regarding express consent for the Education Class.

The individualized questions with respect to consent, which will likely be Google’s principal affirmative defense, are likely to overwhelm any common issues. Therefore, the Court cannot conclude that Plaintiffs have met their burden of demonstrating that the proposed Classes satisfy the predominance requirement.

Editor’s Note: The plaintiffs’ lawyers are seeking immediate Ninth Circuit review of the district court’s decision regarding certification, largely on the ground that that decision was based on a manifestly erroneous view of the possible sources for implied consent (see attached briefs of plaintiff and defendant). This case could set an important precedent regarding the issue of implied consent, with implications for the viability of internet user class actions where the claims are that the internet service provider or website operator obtained or stored user information without consent in violation of federal and/or state law. Since these sorts of claims typically do not involve significant, per-individual-user damages, and since identification and joinder of individual internet users is very resource-intensive, these claims may never be brought if class certification is not available.

* * *

CONSUMER PROTECTION LAWS; STANDING; CHOICE OF LAW


**Plaintiffs Allegedly Defrauded By Dating Website That Misrepresented Confidentiality of Member Information Unable To Establish Standing Under California Unfair Competition and Consumer Remedies Statutes**

Plaintiffs claiming the defendant fraudulently misrepresented the confidentiality of member information on its dating website by omitting the fact that members’ profiles were replicated on affiliate sites were unable to establish standing under California’s Unfair Competition and consumer remedies statutes. Granting the defendant’s motion to dismiss with leave to amend, District Judge Koh held that the plaintiffs had failed to allege what, if any, of the purported misrepresentations the two named plaintiffs actually read. The plaintiffs also failed to allege how knowledge of the defendant’s omissions about affiliate sites would have impacted their decisions to register at the dating website.

The complaint also was unclear whether the plaintiffs suffered any injury. While one of the plaintiffs apparently obtained a paid membership, the complaint did not specify which plaintiff paid, nor did it even make clear that either plaintiff registered on the particular
website where the alleged misrepresentations were made. Most importantly, the plaintiffs failed to make clear that the suffered any economic injury as a result of the alleged conduct. Conclusory allegations of losses of money were insufficient.

The court denied the defendant’s motion to strike the nationwide class allegations. Although the defendant contended California law prohibited application of California consumer protection laws to the non-California plaintiffs, the briefing at the motion to dismiss stage lacked the detail required to conduct the necessary choice-of-law analysis, the court determined.

**Background**

The defendant operated a variety of online dating sites. Among those sites was PositiveSingles.com, which was marketed to persons with sexually transmitted diseases (STDs). The site was designed to help people with STDs meet others who were similarly situated or accepting of members’ medical conditions.

The site allowed individuals to register and create a profile on the site for free. For such individuals, their profile was anonymous. The site also offered paid memberships, and paid members could disclose more information on their profiles and add a picture.

The site’s registration page stated the site was “100% Confidential and Comfortable Community” and that it was free to try out the site. “We do not disclose, sell, or rent any personally identifiable information to any third party organizations.”

The registration page asked members to provide first name, email address, age, ethnicity, height, gender, gender of desired partner, location, and their medical condition. At the bottom of the page, there was a button that created the profile. Just above the button was a check box that states that the member was over 18 years old and had read the “Service Agreement and Privacy Policy,” with a link to the agreement. It stated:

> to expand the availability of profiles on SuccessfulMatch sites, profiles *may* be shared with other sites within the SuccessfulMatch network. By posting or maintaining a profile on this or any other SuccessfulMatch Network site, you agree and consent that said profile shall be subject to placement on other SuccessfulMatch Network sites, at the discretion of SuccessfulMatch, without further notice.

The defendant, in addition to operating its own dating websites, allowed “affiliate partners” to create new online dating websites for niche audiences. The affiliates contracted with the defendant to provide a domain name, a site, and the defendant’s central membership database. Because the defendant managed a single database of member information for all of its sites, a member who registered with an affiliate site could view the profile information of a PositiveSingles.com member.
The defendant allegedly fraudulently and deceptively failed to disclose that profiles created through PositiveSingles.com could be viewed on the affiliate dating sites. While PositiveSingles.com appeared to be a stand-alone site, the defendant allegedly induced people to sign up for the dating service by misrepresenting the privacy of their information. Even if members generally were aware of the existence of the affiliate sites, it was not possible to determine exactly how many and what types of sites were associated with PositiveSingles.com.

Standing

California’s Unfair Competition Law (UCL) prohibits “any unlawful, unfair or fraudulent business act or practice.” California’s Consumer Legal Remedies Act (CLRA) prohibits a host of unfair and deceptive practices, including various forms of misrepresentation. Both the UCL and the CLRA prohibit not only affirmative misrepresentations, but also material omissions that deceive reasonable consumers.

The plaintiffs contended that the defendant violated the unfair and fraudulent prong of the UCL through both affirmative misrepresentations regarding the privacy of users’ profiles on PositiveSingles.com, and through the omission of material facts regarding the sharing of information across the various SuccessfulMatch affiliate websites. In addition, the plaintiffs contended that through these same misrepresentations and omissions, the defendant violated the CLRA. The plaintiffs finally contended that the defendant violated the unlawful prong of the UCL, which incorporated violations of other statutes, because the defendant violated the CLRA.

Both statutes required that plaintiffs demonstrate standing. For the CLRA, this meant allegations of the plaintiff’s reliance on the defendant’s alleged misrepresentation and a resulting injury. Likewise, under the UCL, a plaintiff had to show an injury in fact and the loss of money or property as a result of the unfair competition.

When the unfair competition consists of a defendant’s misrepresentation, the plaintiff must have actually relied on the misrepresentation and suffered an economic injury as a result. While a plaintiff need not demonstrate that the defendant’s misrepresentations were the sole or even the predominant or decisive factor influencing his conduct, the misrepresentations must have played a substantial part in the plaintiff’s decision-making.

For a plaintiff to bring UCL and CLRA claims on the basis of omissions, the omission must either be “contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose.” To establish the causal nexus between the omission and the harm, plaintiffs had to plead that they would not have purchased the product or service if they had known the material fact that the defendant allegedly omitted.
The gravamen of the plaintiffs’ claims under the UCL and CLRA was that the defendant fraudulently misrepresented the confidentiality of member information by omitting the fact that members’ profiles were replicated on the network of affiliate sites. This omission induced individuals with STDs—who had a strong interest in keeping their medical information private—to sign up for the defendant’s dating service. To demonstrate standing under the UCL and CLRA under this theory, the plaintiffs had to allege that they actually relied on the defendant’s misrepresentations and suffered economic injury as a result of that reliance.

The plaintiffs did not rely on any of the alleged misrepresentations on the PositiveSingles.com website. While the complaint and supporting exhibits described representations made on the homepage and registration page, the complaint lacked allegations of what, if any, purported misrepresentations the two named plaintiffs actually read. The plaintiffs failed to specifically allege that they saw any of the statements they claimed were misleading, or how the statements impacted their decisions to register with the website.

Generalized allegations that the defendant had “preyed on the vulnerability” of those who tested positive for STDs and “lured” them with “empathetic sounding statements” were insufficient. At a minimum, the plaintiffs had to allege that they actually viewed the representations that they now contended were misleading.

Further, the plaintiffs had not pleaded any facts to meet the “but for” test for fraudulent omissions. They failed to allege how knowledge of the omissions about affiliate sites would have impacted the plaintiffs’ decision to register for PositiveSingles.com.

The plaintiffs relied on two California cases for the proposition that, in cases involving omissions, an allegation that the omission was material was sufficient without any independent allegation of reliance. But the cases addressed the actual reliance requirements for unnamed class members not named plaintiffs. Neither case purported to excuse named plaintiffs from the pleading requirements necessary to establish standing under the UCL and CLRA.

The complaint also was unclear whether the plaintiffs suffered any injury. Interpreted in a light most generous to the plaintiffs, the complaint and accompanying exhibits supported the inference that one of the two plaintiffs was a paid member of PositiveSingles.com. The exhibits were screenshots of one of the plaintiff’s profiles on different affiliate sites, and the profiles included a picture, suggesting a paid membership.

The complaint failed, however, to specify whose profile was shown in the exhibits, and did not specified whether the other named plaintiff signed up for PositiveSingles.com. Moreover, the complaint did not even make clear that either plaintiff registered with PositiveSingles.com directly. Rather, it was equally possible that the plaintiff whose profile
appeared in the exhibits registered for one of the other affiliate sites. Because the crux of
the plaintiffs’ theory of harm stemmed from misrepresentations and omissions made on the
PositiveSingles.com home page and registration page, the plaintiffs should identify with
particularity on which of the sites the plaintiffs registered.

Most importantly, the plaintiffs failed to make clear that they suffered any economic
injury as a result of the defendant’s conduct. Conclusory allegations of the loss of money
without anything explicit about how the losses were sustained were insufficient.

**Motion To Strike**

The defendant moved to strike the plaintiffs’ nationwide class allegations. According
to the defendant, California’s choice-of-laws analysis under **Mazza v. American Honda
Motor Co.**, 666 F.3d 581 (9th Cir. 2012) prohibited application of California’s consumer
protection laws to non-California plaintiffs in this case. The plaintiffs responded by noting
that the defendant’s Terms of Service required application of California law. The plaintiffs
also asserted that choice-of-law analysis had to be made on a developed factual record, not
a motion to dismiss.

The court said it agreed with the plaintiffs’ latter point. Striking the nationwide class
allegations at this stage in the case would be premature. **Mazza**, which was decided at the
class certification stage, depended heavily on a detailed choice-of-law analysis that com-
pared how various states’ consumer protection laws applied to the facts of the plaintiffs’
claims. Here, the briefing lacked the detail necessary to conduct such an analysis.

The defendant, which had the burden of showing that foreign law, rather than California
law, should apply to class claims in a California choice-of-law analysis, provided no sup-
port for its position that foreign law conflicted with California law, let alone that the con-
lict was so severe as to preclude applying California law to the class claims. Absent the
sort of detailed choice-of-law analysis in **Mazza**, the court said it declined to evaluate how
California’s choice-of-law rules affected the class claims at the present stage of the case.

*   *   *

61
Plaintiffs Allegedly Deceived Into Joining Valueless Discount Membership Programs Adequately Alleged Their Private Data Was “Intercepted” While in Transit Under ECPA but Claims Were Time-Barred

Plaintiffs who allegedly were deceived into joining valueless discount membership programs without their consent, resulting in automatic monthly charges to their credit or debt card accounts, adequately pled that their confidential billing information had been “intercepted” under the Electronic Communications Privacy Act (ECPA). While dismissing the ECPA claims of some of the plaintiffs as untimely under the applicable two-year statute of limitations, U.S. District Judge Bryant held the plaintiffs had alleged an “intercept” of their data while it was in transit.

Observing that courts have narrowly construed the Act’s “intercept” requirement as applying only to data in transit, the court noted that the Second Circuit has suggested that it was not persuaded that an interception could only occur while data was in transit, perhaps opening the door to intercepts of stored data. Finding it unnecessary to decide the issue, the court found that the plaintiffs had alleged an intercept of data in transit. They described a process in which their confidential billing data, entered on the websites of the defendant online retailers, would be stored on an online “token” and transferred to the defendants selling the memberships. The court ruled that the plaintiffs had alleged two alternative intercepts: when the plaintiffs entered the information on the retailers’ sites or when it was transferred to the other defendants.

In ruling that some of the plaintiffs’ ECPA claims were time-barred, the court held that, while the “violation” referenced in the statute was the interception, not the injury caused by the interception, the plaintiffs did not need to be on notice of the actual violation. All that was necessary was that they be on notice to inquire about the injury they received. The court concluded that the plaintiffs were put in inquiry notice when they received their credit and debit card statements. For those plaintiffs who received membership charges on their statements more than two years before filing their complaints, their ECPA charges were time-barred.

The court also rejected the plaintiffs’ RICO claims. The court held that the plaintiffs had failed to allege a proper enterprise and had failed to allege with sufficient detail their mail and wire fraud predicates.
Dismissing in part the plaintiffs’ claims under the Connecticut Unfair Trade Practices Act (CUTPA), the court ruled that the plaintiffs had failed to allege how the passing of confidential billing data to the membership seller was unfair or deceptive. This “datapass” to facilitate further purchases could be used fairly. The plaintiffs could have alleged, for example that their data was transferred to the membership seller who then charged for products never advertised, but the plaintiffs did not do so. The court denied the motion to dismiss, however, to the extent the plaintiffs claimed violations with respect to the defendants’ attempts to minimize refunds to the plaintiffs.

Nevertheless, the court held that the plaintiffs could not bring CUTPA claims as a nationwide class action. The statute barred class action claims by plaintiffs who were not residents or injured in the state. Because this restriction was substantive rather than procedural, Rule 23 could not supersede it.

**Background**

The defendants Trilegiant Corporation, Inc., and its parents Affinion Group, LLC, and Apollo Global Management, LLC (collectively, the “Trilegiant defendants”), allegedly engaged in deceptive, unfair, and fraudulent business practices, enrolling the plaintiffs in “discount” membership programs without their knowledge or explicit consent. These memberships allegedly remained extant for months, and in some cases, for years.

Trilegiant marketed the memberships in collaboration online retailers, the E-Merchant defendants. Trilegiant and the E-Merchant defendants allegedly engaged in post-transaction marketing by creating a false and deceptive appearance, implying that Trilegiant’s offers for membership programs were part of customers’ original transactions with the online retailers. The defendants allegedly placed an offer page between the retailer’s checkout page and its purchase confirmation page; used pop-up windows detailing the membership offers; and provided an enrollment banner on the retailer’s confirmation page.

The E-Merchants also allegedly engaged in “datapass” with Trilegiant, passing customers’ confidential billing information to Trilegiant without the customers’ explicit consent or knowledge. This process allegedly was meant to facilitate further online purchases by relieving customers of the need to reenter credit card or debit account information to complete a secondary transaction with Trilegiant.

The transfer allegedly occurred when a customer clicked on a link that led to Trilegiant’s disguised offer page—presumably before the customer accepted Trilegiant’s offer. After customers unknowingly agreed to purchase Trilegiant’s product, they were returned to their original purchase and received a confirmation only of the original online transaction
with the retailer. Trilegiant then used the transferred billing information to begin charging a monthly membership fee.

Trilegiant allegedly practiced negative option billing. Customers automatically were charged the monthly membership fee unless they took affirmative steps to cancel the membership. This practice allegedly was disclosed in “exceedingly fine print” on Trilegiant’s offer page.

Finally, when customers realized months or years later that they had been charged an illegitimate monthly membership fee, the defendants made it nearly impossible to obtain a full refund through a “refund mitigation strategy.” The E-Merchant defendants allegedly were directly involved.

Call center employees allegedly used several stall tactics to frustrate attempts to cancel memberships and receive refunds, including quickly canceling without a refund and demanding that cancellation requests be in writing. Refunds were limited to a maximum of two months’ fees, unless the caller used words such as “fraud,” “attorney,” “attorney general,” or “lawsuit,” which could lead to a full refund.

The scheme allegedly was possible only with the willing participation of the Credit Card defendants, who ultimately were responsible for processing the charges. The plaintiffs asserted that these defendants were knowing participants by either intentionally or recklessly ignoring their own policies and their own sophisticated anti-fraud software when reviewing and processing membership charges.

The plaintiffs asserted claims for violations of RICO, the ECPA, and the CUPTA, and for unjust enrichment. The defendants moved to dismiss.

**Interception of Data Under ECPA**

The ECPA provided a civil action against persons who intentionally intercept, endeavor to intercept, or procure others to intercept electronic communications. Courts have narrowly defined the term “intercept” to encompass only acquisitions of communications that were contemporaneous with transmissions, not storage. While the Second Circuit has not ruled definitively on the issue, it implied in dictum in *Hall v. Earthlink Network, Inc.*, 396 F.3d 500 (2d Cir. 2005) that it was not persuaded that an interception could occur only during transit.

It was not necessary to decide the issue. Even assuming the defendants’ standard was correct, the plaintiffs sufficiently alleged the temporal requirement.

Several plaintiffs claimed that while making purchases on E-Merchant Defendants’ websites, entered their confidential billing information which then was stored in an online
token to be transferred to Trilegiant at some point in the transaction. They alleged that, after entering their account information, they were taken to Trilegiant’s offer page to complete a secondary purchase without receiving confirmation that the first transaction was completed. They allegedly would receive confirmation of their initial purchase only after reviewing Trilegiant’s offer page.

Based on these allegations and drawing all inferences in the plaintiffs’ favor, the plaintiffs have alleged two alternative “interceptions.” The first could have occurred when the token stored the plaintiffs’ confidential billing information. The interception would have occurred the moment the information was sent to the E-Merchant Defendant, thereby occurring contemporaneously with the communication’s transmittal. An interception did not require immediate use of the intercepted information, so it was irrelevant that the token may only have saved the data.

The second interception could have been when the billing information was sent to Trilegiant. In interpreting “interception” narrowly, courts were only distinguishing between communications that were in transit or in storage. The plaintiffs’ billing information would not have been in storage until after the entire transaction with the E-Merchant was completed, and the online purchase was completed only when the customer received a confirmation page from the vendor.

**ECPA Statute of Limitations**

The applicable statute of limitations for an ECPA claim according to 18 U.S.C. § 2520(e) was “two years after the date upon which the claimant first had a reasonable opportunity to discover the violation.” Courts in the District of Connecticut have held that the merest inquiry notice was sufficient to start the limitations period running absent allegations of fraudulent concealment.

Contrary to the plaintiffs’ contention, they need not be on notice of the actual “violation,” but simply on notice to inquire about their injury. Their credit and debt card account statements should have alerted them that something was going on. Had they inquired about the injury, they would have discovered the alleged violation.

The court said it construed the complaint to allege that the Trilegiant membership fee appeared on the plaintiffs’ credit card statements issued in the month immediately following their enrollment in the program. Thus, the statute of limitations applied to the ECPA claims of plaintiffs who alleged they incurred membership charges more than two years prior to filing their complaints. None of these plaintiffs alleged any irregularity in the customary posting of credit card charges.
Class Action Prohibition

The plaintiffs alleged that the defendants violated the CUTPA by engaging in unfair and deceptive acts and practices. The defendants moved to strike the pleadings related to the CUTPA class action claim because CUTPA did not allow for a class action when a Connecticut resident was not a named plaintiff. The court concluded that the terms of CUTPA and the state’s jurisprudence prohibited the plaintiffs from bringing a class action on behalf of a national class.

Although the plaintiffs argued that the motion was untimely and procedurally improper, the court disagreed. It was not necessary to await a motion for class certification to strike class allegations because the alleged bar to the class proceeding was a statutory restriction unrelated to the issues to be addressed at the class certification stage, namely, those listed in Rule 23. Moreover, the availability for a foreign-named plaintiff to represent a class under CUTPA was a matter of law and could be determined on the fact of the complaint.

Turning to the merits, the court explained that CUTPA created both individual and class causes of action. Persons authorized to bring CUTPA actions on their own behalf are authorized to bring a class action only on behalf of similarly situated residents of Connecticut or those that were injured in Connecticut.

Without arguing that the statute was ambiguous, the plaintiffs asserted on public policy grounds that, although they were not Connecticut residents or injured there, they should be allowed to bring a class action because there was a sufficient nexus to Connecticut: the defendants were headquartered in the state and it was from there that they implemented their scheme. But the court said it could not substitute its judgment for that of the legislature. Moreover, if a statutory analysis were conducted, the statutory language was clear, and the language expressed a deliberate legislative intent that class suits not be permitted, as reflected in the legislative history.

Rule 23 did not supersede the CUTPA class action restriction. In *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393 (2010), a plurality held that Rule 23 trumped a New York statute that precluded any claim with the ability to recover a “penalty” from proceeding as a class action. In a concurring opinion, Justice Stevens clarified that Rule 23 controlled only if the conflicting state law was also procedural, and concluded that the New York statute was procedural. Although the Second Circuit has not addressed which opinion was controlling, several other courts concluded that Justice Stevens’s opinion was controlling because it was decided on the narrowest grounds.

Some courts, either implicitly or explicitly, have bifurcated the *Shady Grove* analysis into two steps. The first is governed by Justice Scalia’s plurality opinion and required a
determination of whether the rule in question was procedural. The second step was to determine whether the state statute was procedural. This method took into account that five justices and the four dissenting justices agreed that a federal rule could not alter substantive rights under state law, and disagreed with Justice Scalia’s broader view that the federal rules superseded both substantive and procedural state laws.

Here, it was clear that Rule would permit a non-Connecticut resident to serve as a named plaintiff of a class action, and the Supreme Court already has determined that the rule was procedural. Second, the CUTPA class action restriction was substantive. The restriction applied only to CUTPA, and nationwide class actions still were possible under other causes of action, such as unjust enrichment. Moreover, the restriction was incorporated into the same sentence that granted the rights of residents and those injured in the state to bring a class action. And, there was at least some evidence to suggest that the decision to restrict class actions was a purposeful policy decision.

Unfair Trade Practices

In alleging CUTPA violations, the plaintiffs asserted that the Trilegiant defendants employed several business and marketing tactics in a deceptive or unfair manner with the aid of the E-Merchant defendants and the Credit Card defendants. These practices included sharing confidential billing information through datapass, employing negative option billing, and making it difficult for consumers to get refunds through the refund mitigation policy.

Datapass was described as the transaction that occurred when confidential billing information was sent to Trilegiant to facilitate further purchases because the customer was not required to reenter credit card information. Negative option billing was the practice in which members automatically were charged a monthly membership fee until they affirmatively cancelled their membership.

The complaint failed to explain how either of these practices was unfair or deceptive. Indeed, it conceded that the negative option practice was disclosed in fine print on the Trilegiant offer page. And, Datapass was not inherently unfair—it allowed customers to complete efficiently several online purchases—but it could be used unfairly.

The plaintiffs had not alleged how datapass was used in an unfair or deceptive manner towards them. Had they alleged that it was used to transfer private billing information to Trilegiant, which then charged for products never advertised, it may have been an unfair or deceptive use of the tool, but no such allegations were made. By pleading only nebulous facts and inferences, the plaintiffs have only provided conclusory allegations and have not sustained their burden on a motion to dismiss.
The plaintiffs have made sufficient allegations, however, to show that the refund mitigation strategy could have violated CUTPA. Call center employees allegedly were instructed to tell customers that they somehow signed up for the membership programs through their credit card company instead of telling them the truth about their membership enrollment.

Assuming these allegations were true, the call center employees were directed to, and did deceive customers who called to cancel their memberships. This misdirection would have permitted Trilegiant to charge more monthly fees while customers attempted to discover how to cancel their memberships. Hence, the claim was actionable under CUTPA.

**CUTPA Statute of Limitations**

The defendants argued that several of the CUTPA claims were time-barred because some of the plaintiffs enrolled in membership programs more than three years before filing their complaints. The plaintiffs responded that they suffered recurring injuries from unauthorized monthly charges, thereby tolling the three-year statute of limitations.

The three-year statute of limitations was an occurrence, not a discovery statute. It began to run at the moment the alleged act or omission occurred. The limitations period began to run from the occurrence of the violation, not the occurrence of the injury. The plaintiff did not even need to have constructive knowledge of the violation for the time period to run.

There were two categories of business practices that the plaintiffs alleged violated CUTPA. The first were those related to the alleged fraudulent enrollment into a membership program. Assuming that this group was not already dismissed for insufficient pleading, the alleged practices were completed, at the latest, by the time the first or second membership fee was posted. Thus all these claims were untimely because the postings occurred more than three years before the complaints.

The second category was the refund mitigation practices. These began only after the plaintiffs discovered the charges and called Trilegiant to cancel their membership or request a refund. Because the plaintiffs alleged that the only discovered the charges and contacted Trilegiant within three years of filing their complaints, the claims were timely.

The plaintiffs asserted that the continued injury of monthly membership fees tolled the statute or limitations, or alternatively, that they could recover for damages that occurred within the three-year period. But they failed to allege sufficiently how charging a recurring monthly membership fee that clearly was listed on credit card statements violated CUTPA. Moreover, these actions constituted only a repeating injury, not a recurring violation. Because the plaintiffs alleged that the datapass and failure to disclose the negative
option billing practice occurred more than three years ago, any damages resulting from those injuries no longer were compensable.

The plaintiffs’ reliance on the fraudulent concealment doctrine to toll the limitations period was unavailing. The plaintiffs had notice of the alleged fraud when they received their account statements. Indeed, the submission of the statements to the plaintiffs actually revealed, rather than concealed, the membership charges.

Finally, the continuing course of conduct doctrine was of no help to the plaintiffs. Under Connecticut law, the doctrine did not apply in a vendor-vendee relationship if the plaintiff did not allege a continued pattern of deceitful conduct after the initial fraud because a vendor was under no legal obligation to disclose its initial deceitful conduct. The plaintiffs needed to allege a continuing pattern of behavior, but once the plaintiffs were enrolled in the membership program, they immediately were put on notice of their enrollment and the continuing fees. The plaintiffs had not alleged that the listed charges were themselves inaccurate or fraudulent.

### Unjust Enrichment

Under Connecticut law, plaintiffs asserting unjust enrichment claims had to show that the defendants were benefitted, that the defendants unjustly did not pay the plaintiffs for the benefits, and that the failure to pay was to the plaintiffs’ detriment. The plaintiffs alleged that the defendants tricked them into enrolling in a membership program, and then automatically charged them recurring membership fees; when the plaintiffs discovered they were being charged, the defendants would make it very difficult for them to obtain a refund. The court concluded that, at the motion to dismiss stage, the plaintiffs had sufficiently pled their unjust enrichment claim as to Trilegiant and the E-Merchant defendants.

As part of the refund mitigation strategy, the E-Merchant defendants were heavily involved in organizing and implementing the tactics. Trilegiant allegedly paid these defendants signing bonuses and sizeable percentages of each dollar collected from their customers.

The plaintiffs failed, however, to sufficiently allege how the Credit Card defendants were involved in the scheme or unjustly enriched. The plaintiffs admitted that Trilegiant conducted legitimate business selling membership programs through lawful means, and the plaintiffs did not allege how the Credit Card defendants would have known which members were willing participants and which felt they were fraudulently enrolled.

The assertion that these defendants reviewed Trilegiant’s call-center scripts and participated in calls with customers seeking a refund did nothing more than explain that these
defendants were taking their customers seriously. Further, unlike the E-Merchant defendants who shared in the alleged scheme’s proceeds, the Credit Card defendants allegedly were engaged in the ordinary course of business by processing charges at their standard processing fee for all of their customers.

* * *

VIDEO PRIVACY PROTECTION ACT; CLASS ACTION

_in re Hulu Privacy Litigation_, No. C 11-03764 LB (N.D.Ca. April 28, 2014)

Federal Court Dismisses VPPA Claims Based on Video Viewing Data Disclosed to Metrics Company but Allows Claims for Disclosures to Facebook Finding That Users Could Have Been Linked to Facebook Accounts

On April 28, 2014, U.S. Magistrate Judge Beeler of the federal district court for the Northern District of California, San Francisco Division, granted in part and denied in part, video website defendant Hulu’s motion for summary judgment. Hulu users brought a class action against Hulu alleging that it violated the Video Privacy Protection Act by disclosing their personally identifiable information to a metrics company and Facebook. The Court dismissed the claims based on disclosures to the metrics company upon finding that the plaintiffs failed to show that the metrics company used unique Hulu-assigned user ID numbers to link video watching data with Hulu user profiles that included user names. On the other hand, the Court allowed claims to proceed based on the disclosures to Facebook finding that Hulu coding automatically caused Hulu users’ browsers to transmit information to Facebook that revealed video data, and could have allowed Facebook to link the user to a Facebook user account.

Background

A group of registered Hulu users (Plaintiffs) brought a class action against the on-demand video website Hulu. Plaintiffs alleged that Hulu violated the Video Privacy Protection Act (VPPA) by sharing certain personally identifiable information (PII) of Hulu users with a metrics company called comScore, and the social network Facebook.

Hulu required users to establish a user profile when they first registered for the service, and assigned each user a unique seven-digit Hulu User ID. That User ID appeared in unencrypted form in the URL web address of the user’s profile page. The profile page also included the user’s first and last name.

Hulu sent user information, including User IDs, to comScore in order to use its metrics to track and analyze Hulu usage. The information generated was used to procure additional
programming and advertising. The reports generated by comScore never identified users by name, and instead presented data in an aggregated and generalized basis with no reference to User IDs linked to profile pages. However, comScore was provided the User IDs and could hypothetically, through reverse engineering, use User IDs to gain access to Hulu user profile pages. Hulu also provided comScore with a cookie that included a unique comScore ID assigned to each Hulu user. The cookie allowed comScore to track other websites visited by Hulu users.

Hulu also transmitted Hulu user information directly to Facebook via the Facebook “Like” button. Hulu included a Facebook Like button on each Hulu webpage. When the Hulu user visited the website, the browser automatically executed a code that loaded the Like button on the Hulu page. When this was done, the IP address of the registered user’s computer was sent from Hulu to Facebook. Hulu also sent various cookies to Facebook which allowed Facebook to link the Hulu user’s video usage to a Facebook user ID and account which likely contained identifying data. This was all done automatically and did not require the Hulu user to click on the Like button.

Hulu moved for summary judgment arguing that it only disclosed anonymous user IDs and never linked them to identifying data, and that it did not disclose information knowingly as required under the VPPA.

The VPPA Prohibits Disclosures That Tie Specific People to Videos They Watch

The VPPA prohibits a videotape service provider from knowingly disclosing personally identifiable information (PII) concerning any consumer of such provider.

The Court had to first decide whether Hulu’s disclosures here were considered PII as defined by the VPPA. It analyzed the plain meaning of the statute and found that it was ambiguous as to whether it covers unique anonymous user IDs like the Hulu User IDs here. It then looked to the legislative history of the Act and found that the Congress intended the statute to plainly encompass others means of identifying a person. Disclosing a user’s name was just one method by which a user’s PII can be shared. Case law also supported the proposition that an anonymous unique ID, without more, does not constitute PII, but that if it is disclosed to a person who could understand it, it might constitute PII covered under the Act.

Accordingly, the Court held that the VPPA protects PII that identifies a specific person and ties that person to specific videos that the person watched. While an anonymous unique ID alone may not be enough to constitute PII, analyzing the user ID in context could render it the equivalent of the identification of a specific person, which may be actionable under the VPPA.
Disclosures to Metrics Company Not Sufficient To Allow VPPA Claims

Applying this standard, the Court dismissed Plaintiff’s claims based on Hulu’s disclosures to comScore. Plaintiffs’ claims were based on the hypothetical that comScore could use the Hulu ID to access a Hulu user’s profile page and obtain the user’s name. However, Plaintiffs failed to present any evidence that comScore did in fact do this so as to give rise to a claim under the VPPA. For the same reason, the Court found that the cookies sent by Hulu to comScore did not amount to a VPPA violation because there was no evidence that comScore’s tracking of users’ visits to other websites necessarily revealed a specific identified person’s identity and viewing history.

Disclosures to Facebook Were Sufficient To Allow VPPA Claims

On the other hand, the Court denied Hulu’s motion for summary judgment as to Plaintiffs’ claims relating to disclosures made to Facebook because questions of material facts remained as to whether the cookies sent from Hulu to Facebook amounted to an actionable disclosure of PII. Hulu sent data through cookies automatically to Facebook at the same time that a user loaded a page with a video. This allowed Facebook to link the Hulu user to an existing Facebook user account when it received this disclosure from Hulu. The cookies taken together revealed information on what the user watched and simultaneously could have been used to identify the user.

The Court also relied on the fact that this was a Hulu-initiated automatic transmission of information. The interaction between the two websites was a Hulu-prompted request from the Hulu user’s browser to Facebook to load a Like button the screen. Because this allowed Facebook to link that user to a Facebook user account and profile, this was not the mere transmission of a unique anonymous ID. The Court noted that, had this transmission happened only when the user clicked on the Like button rather than automatically, the claims would not have been actionable under the VPPA.

Meaning of “Knowingly” Under the VPPA

Hulu also argued that these disclosures were not done knowingly as is required for a claim under the VPPA. No court had previously interpreted the term “knowingly” under the VPPA. Upon analyzing similar privacy statutes, the Court held that the term here means “consciousness of transmitting the private information.” Therefore, the test here was whether Hulu knew that Facebook might attempt to read the cookies identifying the Hulu videos being watched together with the Facebook cookies that linked the Hulu user to a Facebook account. There was some evidence in emails suggesting that Hulu was concerned about this possibility and about VPPA violations. This was sufficient to demonstrate
that factual issues remained for trial. Accordingly, the Court denied Hulu’s motion for summary judgment.

*   *   *

STANDING; PLEADING; CA UNFAIR COMPETITION LAW

_In re LinkedIn Privacy Lit.,_ Case No.: 5:12-CV-03088-EJD (N.D. Ca. Mar. 28, 2014)

Federal Court Finds Plaintiff Has Standing To Bring Claims Because California’s Unfair Competition Law Defines “Advertisement” Broadly Enough To Encompass Alleged Misrepresentations in LinkedIn’s Privacy Policy

Judge Davila writing for the federal court for the Northern District of California, San Jose Division granted in part and denied in part, LinkedIn’s motion to dismiss a class action lawsuit alleging violations of the California Unfair Competition Law (UCL). The court found that the plaintiff had standing to bring a UCL action in federal court because plaintiff sufficiently alleged that LinkedIn’s representations were false. A consumer who alleges she was induced by misrepresentations to purchase a product the consumer would otherwise not purchase has standing to bring a claim, even if the relevant portion of the privacy policy might only be significant only to a small segment of consumers.

Background

Khalilah Wright (Plaintiff) brought a putative class action against LinkedIn Corporation. LinkedIn owns and operates the website www.LinkedIn.com, an online community for professional networking. When prospective members register for the service, they are required to confirm that they agree to LinkedIn’s User Agreement and Privacy Policy. The Privacy Policy contains a statement that “all information that you provide will be protected with industry standard protocols and technology.” A paid “premium” subscription grants prospective members increased networking tools and capabilities. Premium subscribers agree to the same terms and services of the User Agreement and Privacy Policy as non-paying members.

Plaintiff alleged that, in 2012, LinkedIn’s computer systems were hacked. The hackers posted approximately 6.5 million stolen LinkedIn users’ passwords on the Internet. LinkedIn subsequently announced that it had completed a switch of its password encryption method from a system that stored member passwords in a hashed format to one that used both salted and hashed passwords for increased security.

The Court dismissed without prejudice Plaintiff’s first complaint for lack of Article III standing, finding the promise of industry standard security had not been a part of Plaintiff’s
bargain for premium services. Plaintiff then brought a Second Amended Complaint (SAC) alleging that she paid for a premium subscription from March 2010 until approximately August 2010 and that her password was retrieved by the hackers and posted on the Internet on June 6, 2012. She also alleged that, prior to her purchase of the premium subscription, she read LinkedIn’s User Agreement and Privacy Policy and that, had LinkedIn accurately disclosed its security practices, she would have viewed the premium subscription as less valuable and would have declined to purchase a premium subscription or she would have done so at a lower price. She brought a claim for violation of the fraudulent business practices prong of California’s Unfair Competition Law (UCL), Cal. Bus. & Prof. Code, § 17200 et seq.

LinkedIn moved to dismiss arguing Plaintiff lacked standing under Article III of the U.S. Constitution and the UCL, failed to state a claim under Rule 12(b)(6), and failed to plead fraud with sufficient particularity.

Standing

Plaintiff contended that she had standing because she purchased her premium subscription in reliance on LinkedIn’s misrepresentation and would not have done so but for the misrepresentation. Plaintiff alleged that she read and relied upon the statement in the Privacy Policy regarding industry standard security. With these amendments, the court found the SAC’s allegations sufficient to confer standing under Article III and statutory standing under the UCL.

Plaintiff argued that standing under the UCL and under Article III can be established by allegations that she relied on a misrepresentation contained in the Privacy Policy and she would not have bought the product but for the misrepresentation. She relied primarily on a line of cases in which courts found standing for plaintiffs who purchase deceptively labeled or advertised products in reliance on the misinformation contained in the labels or advertisements. LinkedIn argued that one sentence in the Privacy Policy could not be considered inducement to the purchase a premium subscription, the advertisement of premium services, or an effective marketing technique for premium service. It also argued that Plaintiff’s allegations failed to establish injury in fact because they were premised on the payment or overpayment for a product. Courts have required plaintiffs to allege “something more” than “overpaying for a ‘defective’ product” in order to establish an Article III injury in fact.

Although the court recognized that there are significant differences between the “single sentence” contained in Defendant’s Privacy Policy and the representative cases regarding labels and advertisements, the court found the representation in LinkedIn’s Privacy Policy fell within the scope of the labeling/advertising cases. Not only did case law not limit
misrepresentations to labels or advertisements, but the term “advertisement” is broadly defined under California law. The UCL incorporated the Fair Advertising Law’s prohibition on unfair advertising as only one form of unfair competition. The court found that establishing one standing standard to advertising and another for other types of misrepresentations would be untenable given the lack of distinction California law places between misleading advertising and other forms of misleading statements.

Although LinkedIn’s Privacy Policy might only be significant to few consumers and many may not even read it, when such a statement contains false representations, a consumer who is induced by them to purchase a product that she otherwise would not have purchased has standing to bring an action under the UCL in federal court. Applying the cases discussed above, the Court found Plaintiff’s allegations sufficient to establish standing under the UCL and Article III.

Rule 12(b)(6)

To state a claim under the fraudulent business practices prong of the UCL, a plaintiff must only show that members of the public are likely to be deceived. LinkedIn argued that Plaintiff’s claims should fail because it was implausible that a single sentence in a Privacy Policy was likely to deceive the public. However, the Court did not find Plaintiff’s claims were barred as a matter of law because she alleged that if Defendant had disclosed its security protocols, consumers would have learned that the protocols did not meet industry standards though other sources.

Rule 8

LinkedIn argued that the SAC did not satisfy Rule 8, requiring that a complaint contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” It contended that because some of Plaintiff’s allegations regarding the incorporation of the User Agreement into the Privacy Policy were false, the Court should not accept as true Plaintiff’s allegations that she read and relied on the Privacy Policy in purchasing her premium subscription. The Court found that Plaintiff’s understanding of the legal incorporation of the User Agreement was immaterial and Plaintiff sufficiently alleged that she read and relied on those documents.

Defendant also argued that Plaintiff’s allegation that Defendant failed to use industry standards to encrypt member passwords was conclusory and unsupported. The Court declined to dismiss the claim, finding Plaintiff’s allegations were sufficient to support her allegations of false representation because she was specific about the particular security practice that Defendant used and alleged that those practices fell below the minimum industry standards.
Rule 9

The Court also found Plaintiff’s allegations implicating fraud met the particularity requirements of Rule 9(b) because she alleged that the representation was made in Defendant’s Privacy Policy, which she read and relied on prior to purchasing a premium subscription, and she alleged facts that explain why the representation was false.

*  *  *

CFAA; DAMAGE; LOSS; TRADE SECRETS; EMAIL; MOTION TO DISMISS


**Federal Court Holds That the Costs of Investigating Theft of Trade Secrets By Means of Unauthorized Copying of Email Was Not a “Loss” Under the CFAA**

In this suit by a company employer against a former employee who allegedly copied emails containing trade secrets before leaving the company, the Court dismissed the Computer Fraud and Abuse Act (CFAA) claim. The Court acknowledged that the company had incurred costs in investigating what the former employee had copied and what the implications of that copying might be for its business. But the company lost no data, and its investigation was not focused on determining the loss of any data. Under these circumstances, the company’s investigation costs did not qualify as a “loss” under the CFAA and the Court therefore dismissed the CFAA claim.

Editor’s Note: Although the Court suggests that its interpretation of “loss” under the CFAA is consistent with other court decisions, a number of cases do hold that the costs of investigating the actions of a hacker or unauthorized user of a computer are a “loss” under the CFAA, and the Court did not make any real effort at distinguishing those cases. The Court definition of “loss” under the CFAA appears to be narrower than that adopted by some other decisions.

**Background**

SBS is a global logistics company specializing in international freight and supply chain solutions. Potts began his employment at SBS in May of 1998, and prior to his resignation held the position of Business Development Executive. In this role, he was responsible for finding new customers and interacting with existing customers to increase sales of SBS’s products and services. Beginning in January of 2011, Potts began forwarding emails containing SBS’s confidential customer information to his personal email account, in violation of SBS’s company policy, and continued to do so until his resignation on July 2, 2013. Before he left, Potts attempted to delete the forwarded emails from his SBS email account.
On Saturday, June 15, 2013, Potts entered SBS’s offices and removed a number of SBS files. After his resignation, Potts began working for Woodland, which competes with SBS to provide international freight and supply chain solutions. SBS alleged Potts promised Woodland he would use his knowledge of SBS’s confidential customer information to solicit SBS clients on behalf of Woodland.

**SBS’s Computer Fraud and Abuse Act Claim**

Count IV alleged Potts intentionally—and without authorization—accessed SBS’s computers, intranet, and email system and emailed SBS’s confidential customer information to his personal email account. SBS also alleged Potts attempted to conceal his theft by deleting the outgoing emails from his SBS email account. Notwithstanding Potts’s attempt to cover his tracks, SBS did not allege it lost access to any information as a result of Potts’s conduct. SBS did, however, allege Potts’s conduct caused a “loss” of at least $5,000, including costs related to damage assessment and mitigation.

To state a claim for a violation of the CFAA, a plaintiff must prove: “(1) damage or loss; (2) caused by; (3) a violation of one of the substantive provisions set forth in § 1030(a); and (4) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)-(V).” The “underlying concern of the [CFAA] is damage to data and . . . the statute was not meant to cover the disloyal employee who walks off with confidential information.”

The Court opined that “SBS does not—and cannot—claim Potts’s conduct caused “damage” within the meaning of the CFAA, because SBS does not allege any data were lost or impaired.”

Courts in this district have consistently interpreted ‘damage’ under the CFAA to include ‘the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any diminution in the completeness or usability of the data on a computer system.’ By contrast, downloading and emailing trade secrets is not enough to satisfy the damage requirement of the CFAA.

Instead, SBS alleged it suffered a “loss” attributable in part to damage assessment and mitigation. The CFAA defines “loss” as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). As the Court noted, the interpretation of loss among by courts has varied:

District courts in this circuit have construed the term “loss” in different ways. Compare Farmers Ins. Exch., 823 F.Supp.2d at 854 (“[A] plaintiff can satisfy the CFAA’s definition of loss by alleging costs
reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused no damage as defined by the CFAA.”) (citations omitted), with Von Holdt v. A–I Tool Corp., 714 F.Supp.2d 863, 875–76 (N.D.Ill. 2010) (Manning, J.) (requiring “damage to the computer or computer system” before a plaintiff can prove “loss” under the CFAA). Courts generally agree, however, that “[c]osts not related to computer impairment or computer damages are not compensable under the CFAA.” Farmer Ins. Exch., 823 F.Supp.2d at 855 (quoting SKF USA, Inc. v. Bjerkness, 636 F.Supp.2d 696, 721 (N.D.Ill. 2009) (Pallmeyer, J.)) (additional citations omitted); see also Cassetica Software, 2009 WL 1703015, at *4 (“With respect to ‘loss’ under the FCAA, other courts have uniformly found that economic costs unrelated to computer systems do not fall within the statutory definition of the term.”); CustomGuide v. CareerBuilder, LLC, 813 F.Supp.2d 990, 998 (N.D.Ill. 2011) (Holderman, J.) (finding plaintiff failed to state a CFAA claim by failing to allege “any facts connecting its purported ‘loss’ to an interruption of service of its computer systems”).

Here, SBS did not “allege any facts connecting its purported loss to an interruption of service, loss of data, or even a suspected loss of service or data.” Although SBS attributed certain losses to “damage assessment and mitigation,” it was “clear” from the Complaint that SBS’s “damage assessment” efforts were aimed at determining the scope of information Potts emailed to himself and disclosed to Woodland. SBS did not allege it ever lost access to any of the information contained in Potts’s emails, notwithstanding Potts’s attempt to conceal his conduct by deleting the emails. For the Court, the cost of investigating the competitive injury resulting from illegal copying of alleged trade secrets was not a “loss” within the meaning of the CFAA:

To be sure, assessing the extent of information illegally copied by an employee is a prudent business decision. But the cost of such an investigation is not “reasonably incurred in responding to an alleged CFAA offense,” because the disclosure of trade secrets, unlike destruction of data, is not a CFAA offense. Farmers Ins. Exch., 823 F.Supp.2d at 854. Accordingly, the costs of investigating Potts’s conduct are not “losses” compensable under the CFAA.

“Because SBS’s Complaint fails to allege any damage or loss within the definition of the CFAA, SBS’s Complaint fails to state a violation of the CFAA.” Potts’s motion to dismiss Count IV was thus granted. [Note: the Court did not dismiss the plaintiff’s trade secrets claims.]

*   *   *

78
In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., Magistrate Case. No. 14–228 (JMF) (D. D.C. Mar. 07, 2014)

Federal Court Refuses To Grant Warrant for Materials Associated With an Apple Email Address and Instructs the Government To Narrow Its Search Requests

In a November 2013 opinion, the District Court for the District of Columbia warned the United States Government that it would not tolerate sweeping or unlimited warrant requests for all communications associated with an electronic address, and granted the warrant, but did so only after narrowing the scope of the warrant on its own initiative. In this opinion regarding an Apple email address, the Court again complained that the Government was seeking the entire universe of information tied to a particular account, even though it had established probable cause only for certain information. The Court refused the requested warrant as unconstitutionally vague and broad, and stated the Government needed to, but had not, specified that the initial search could be performed by the electronic service provider and needed to, but had not, explained what would happen to seized email or other materials. The Court therefore denied the warrant request, in an obvious attempt to induce the Government to change its approach to warrants regarding electronic data.

Background

The Government applied for a search and seizure warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), (b) and (c) to disclose certain records and contents of electronic communications relating to an Apple e-mail address. The requested warrant related to an investigation of a possible violation of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy) involving a defense contractor.

The Court Concludes the Government “Seeks an Unconstitutional General Warrant”

The Court explained that it was “increasingly concerned about the government’s applications for search warrants for electronic data.” “In essence, its applications ask for the entire universe of information tied to a particular account, even if it has established probable cause only for certain information.” “Despite the Court raising its concerns and urging the government to adopt a different approach [in previous cases], the government continues to ask for all electronically stored information in e-mail accounts, irrespective of the relevance to the investigation.”
The Court was troubled that the government sought a broad search and seizure warrant for e-mails and all other content related to this e-mail account. “With respect to searches of electronic information, careful attention must be paid to the dictates of the particularity requirements of the Fourth Amendment . . . .” The Government cannot avoid the particularity requirement by claiming it is not seizing material it reviews but then deems irrelevant to its investigation:

The two-step procedure of Rule 41 cannot be used in situations like the current matter to bypass this constitutional reality because the data is seized by the government as soon as it is turned over by Apple. Even if, as Professor Orin Kerr has stated, a search does not occur until “the data is exposed to possible human observation,” Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L.Rev. 531, 551 (2005), the seizure of a potentially massive amount of data without probable cause has still occurred—and the end result is that the government has in its possession information to which it has no right. See In re App., 2013 WL 4647554, at *9 (“The Court notes that while nothing in Section 2703 or Fed.R.Crim.P. 41 may specifically preclude the government from requesting the full content of electronic communications in a specific email account, the Fourth Amendment may do so and does here.”). What the government proposes is that this Court issue a general warrant that would allow a “general, exploratory rummaging in a person’s belongings”—in this case an individual’s e-mail account. Coolidge, 403 U.S. at 467, 91 S.Ct. 2022. This Court declines to do so.

“If a wide disclosure followed by a government search violates the Fourth Amendment, then the obvious answer is to have Apple perform the search using the criteria that the government would itself use in the same way that a bank, in the example used above, might find a particular type of document in its customer files.” The Court was aware that other district courts have held that the “Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.” “But, in light of the government’s repeated submission of overly broad warrants that violate the Fourth Amendment, this Court can see no reasonable alternative other than to require the provider of an electronic communications service to perform the searches.” “Under the government’s demand that it be given everything, the government leaves the Court with only two options: deny the warrants—thus depriving the government of needed information—or issue warrants that are repugnant to the Fourth Amendment.” But “[n]either is viable.” As the Court elaborated:

Thus, having an electronic communication service provider perform a search, using a methodology based on search terms such as date stamps, specific words, names of recipients, or other methodology suggested by the government and approved by the Court seems to be the only way to enforce the particularity requirement commanded by the Fourth Amendment.
The Court was “particularly troubled that the Application does not specify what will occur with e-mails and other information that is, even by the government’s standards, not relevant.” “Will that information be returned, destroyed, or kept indefinitely?” “The “Secondary Orders” that have been routinely issued by this Court—and a significant portion of the Facebook Opinion—have required the government to destroy all contents and records that are not within the scope of the investigation as outlined in the search warrant. See Facebook Opinion, — F.Supp.2d ——, 2013 WL 7856600, at *7.” “While such a clause in a search warrant application is certainly necessary for its issuance by this Court, the government should not believe that it is sufficient.” “In this case, its absence is grounds enough for the Court to deny the Application.” As the Court explained, it felt it had no choice but to deny the warrant application:

By the Court’s count, it modified approximately twenty search and seizure warrants for electronic information during September and December 2013. It will no longer do so. Instead, any warrants that do not comport with the requirements of the Fourth Amendment will—like the present Application—be denied with an explanation of why they have been denied so that the government may have an opportunity to correct its defects. To be clear: the government must stop blindly relying on the language provided by the Department of Justice’s Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual. By doing so, it is only submitting unconstitutional warrant applications.

*   *   *

CFAA; LOSS; WITHOUT AUTHORIZATION; UNAUTHORIZED; MOTION TO DISMISS


Federal Court Holds That Third Circuit Has Not Yet Ruled on the Scope of CFAA Liability and Adopts a Narrow Construction of “Without Authorization” Under the CFAA

This case involved claims by a company that employees used their workplace passwords to access workplace computers and retrieve information that they then shared with a competitor after they left the company. The Court held that the plaintiff had adequately alleged “loss” under the Computer Fraud and Abuse Act (CFAA) but had not adequately alleged that defendants’ accessing of the computer system at issue was “without authorization.” The Court disagreed with the plaintiff that the Third Circuit had adopted a broad construction of “without authorization” under the CFAA, and instead concluded that the Third Circuit had not yet addressed the debate over whether that term means only accessing
a computer that is wholly off-limits to an employee or rather also encompasses situations where the employee had been given access to a computer for certain purposes but then accesses for his or her own potential gain and in order to harm the employer. The Court adopted the narrower interpretation of the scope of CFAA liability, reasoning that the language of the statute, the statute’s anti-hacking purpose and the rule of lenity all supported the narrower interpretation. Because the employer in this case had given the defendants access to the computer system at issue, the Court held that the access was authorized. The Court therefore dismissed the CFAA claim.

Background

Plaintiff owned and maintained a password-protected computer system with a file and email server for use in operating its business, storing confidential company and client information and performing work on client projects. Each defendant had access to this system and plaintiff limited their access for purposes related to client work on plaintiff’s behalf. Upon leaving plaintiff’s employ, each defendant allegedly copied and stole “valuable data from [p]laintiff’s password protected computer system and took that data for use unrelated to his or her subsequent employment [with] [p]laintiff’s competitor.” Plaintiff claimed that defendants had “no authority to access [p]laintiff’s password-protected computer system or the data therein for any other purpose, and any such access for purposes other than serving [p]laintiff was . . . without authorization.”

Plaintiff asserted that defendant’s retrieval and copying of its data was in direct violation of its employee policies. During their employment, each defendant was given and required to comply with plaintiff’s employee handbook, which set forth employee policies regarding confidentiality of client and customer matters, Internet usage, laptop security, work created by employees, protecting company information, conflicts of interest and code of ethics, outside employment and resignation.

The CFAA Claim

Defendants argued that plaintiff’s complaint should be dismissed for failure to allege damage or loss under the CFAA. Section 1030(g) of the CFAA authorizes a private cause of action for any person “who suffers damage or loss by reason of a violation” but “only if the conduct involves [one] of the factors set forth in” subsection 1030(c)(4)(A)(i). 18 U.S.C. § 1030(g) (emphasis added).” Because Section 1030(g) is disjunctive, a plaintiff meets its burden by showing either loss or damage. Here, defendants argued that plaintiff had not properly asserted damage under the CFAA, because the only damages recoverable are (1) the cost of remedial measures taken to investigate and repair damage to the computer system and (2) lost revenue when the damage computer was inoperable.
Plaintiff responded that it has adequately pled the loss requirement of the CFAA. The Court agreed that plaintiff has adequately pled loss, as it explained:

Under the CFAA and persuasive authority authored by our sister courts, plaintiff need not show that their system was rendered inoperable, or that tangible damage was done to their computer system. Plaintiff may show loss by alleging that it expended an amount to investigate whether such damage occurred. . . . Here, plaintiff relies on the “loss” factor under Section 1030(g) rather than the “damage” factor to state a claim under the CFAA. It claims it expended an amount in excess of $5,000 to conduct a computer forensic investigation, analysis and review and to mitigate the data breach, and incurred a loss of productivity due to the in-house investigation of the data breach. Taken these statements as true, as the Court must at this phase, plaintiff has met the required loss element because these are reasonable costs plaintiff expended in responding to the data breach caused by defendants and conducting a damage assessment. Therefore, plaintiff’s complaint will not be dismissed for failure to show loss.

Although plaintiff has adequately plead that it incurred a loss under the CFAA due to defendants’ actions, it must still show that defendants either obtained access to the computer without authorization or exceeded their authorized access when they obtained access to copy the data from plaintiff’s computers. The Court found that defendants neither obtained access to the data without authorization nor exceeded their authorized access in copying the files and plaintiff’s complaint is dismissed for failure to state a claim under the CFAA. As the Court explained, there is a circuit-split that has arisen as a result of divergent interpretations from deciphering the breadth of the term “authorization.” Under the narrow view, an employee given access to a work computer is authorized to access that computer regardless of his or her intent to misuse information and any policies that regulate the use of information. Under the broad view, if an employee has access to information on a work computer to perform his or her job, the employee may exceed his or her access misusing the information on the computer, either by severing the agency relationship through disloyal activity, or by violating employer policies and/or confidentiality agreements. The Court found

that the Court of Appeals for the Third Circuit has not explicitly adopted the broader and majority interpretation, and accordingly finds that the narrow interpretation of the CFAA adopted by the Court of Appeals for the Ninth and Fourth Circuits and by district courts in our circuit is the proper interpretation of the statute and the true interpretation of Congress’ intent in enacting the statute.

The Court elaborated upon its view that the Third Circuit had left this issue open:

The narrow holding [by the Third Circuit] in Tolliver cannot fairly be characterized as an express adoption of the broad interpretation of the CFAA language. The issue in Tolliver was whether the criminal conviction was supported by sufficient evidence. The Court was not asked to address the breadth of the
term “authorization.” Tellingly, the opinion in Tolliver, which was decided in the midst of circuit split described above, did not reference that fact. The Court did not cite to or discuss cases in which the broad view or the narrow view of the language in the CFAA was at issue. Thus, this Court declines to find that the Court of Appeals for the Third Circuit “expressly” adopted the broader interpretation of the CFAA or to extend the holding in Tolliver, especially in light of the non-precedential status of that decision. See In re Grand Jury Investigation, 445 F.3d 266, 276 (3d Cir.2006); Gilmore v. Ford Motor Co., 2013 WL 869382, at *1 (W.D.Pa. March 7, 2013).

The Court found persuasive the reasoning of courts that adopt the narrow view of the CFAA, which is based on “the plain language of the statute, dictionary definition of “authorization,” and the rule of lenity.” As the Court explained:

The Fourth Circuit goes through this analysis for a factual scenario very similar to this case. . . . The [Fourth Circuit] began with examining the plan language of the statute. Id. at 203. It recites the Oxford English Dictionary definition for “authorization”: “formal warrant, or sanction.” Id. at 204. Citing the Ninth’s Circuit’s analysis in LVRC Holdings, LLC v. Brekka, the [Fourth Circuit] concluded that “an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer,” and employee is ”without authorization” when “he gains admission to a computer without approval,” and an employee “exceeds authorized access” “when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access.” . . . These definitions do not extend to the improper use of information validly accessed. Id. at 204. As for an ambiguity surrounding the term “without authorization,” the [Fourth Circuit] noted that its interpretation would apply to both the civil and criminal parts of the statute, and therefore any ambiguity would be resolved in favor of lenity. . . . This rule ensures that we are shielded from unexpected criminal consequences of ambiguous statutes. . . . As a result, the [Fourth Circuit] was “unwilling to contravene Congress’s intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy.”

Here, plaintiff admitted that each defendant was permitted to access its computer system and network and was permitted to access the data at issue. Plaintiff did not allege that defendants “hacked into” a computer or the files that they were not otherwise permitted to access. Rather, the crux of plaintiff’s argument was that defendants lost the right to access such information when they did so for their own or a third parties benefit, and to the detriment of plaintiff. Such a finding would be “contrary to the plain language of the statute” that governs “access” and not “use.” “Plaintiff cannot state a claim under the CFAA by transforming its employee policies which prohibited the using of the computer system for anything other than business purposes into a violation of the CFAA.” “Plaintiff does not claim that defendants gained admission to a computer without its approval or that they used
their access to obtain information that falls outside the bounds of approved access.” “That defendants obtained information that could not have been used for any bona fide business purpose does not fall within the scope of exceeding authorized access if the employee is permitted to otherwise access the data.” Accordingly, the Court dismissed the CFAA with prejudice.

* * *

CFAA; DAMAGE; LOSS; CALIFORNIA UNFAIR COMPETITION LAW; BATTERY LIFE; MOTION TO DISMISS

In re Google Android Consumer Privacy Litigation, No. 11-MD-02264 JSW (N.D. Cal. Mar. 10, 2014)

Federal Court Dismisses CFAA Claim By Google Users Who Alleged Google Collected Their Personal Data Without Permission

In this collection of putative class actions against Google alleging that Google made unauthorized use of the personal data of users of mobile devices, the Court dismissed the Computer Fraud and Abuse Act (CFAA) claim against Google but declined to dismiss the plaintiffs’ claim under California’s Unfair Competition Law. The principal economic harm alleged by the plaintiffs was that Google’s unauthorized collection of the data of the users of mobile devices drained the batteries of their devices. The Court explained that while loss in battery life could constitute “damage” within the meaning of the CFAA, the CFAA requires a showing of $5,000 in damage, and the plaintiffs’ allegations did not support an inference that the plaintiffs incurred damage in that amount. The Court held plaintiffs had stated a claim under California’s Unfair Competition Law by alleging that Google made false statements regarding user privacy and Google’s practices that led plaintiffs to pay more for mobile devices than they otherwise would have paid.

Background

Plaintiffs alleged that Google “gained and allowed third parties to have unauthorized access to, and engaged in unauthorized use of,” their mobile devices, which use Google’s Android Operating System (AOS). According to plaintiffs, they each installed one or more of the following software applications on their Android mobile devices: Foursquare; Groupon; Advanced Task Killer; Angry Birds; and Pandora. Plaintiffs alleged that these Apps “collected personal data from their Android Mobile Phones and shared this data with” Google. Plaintiffs contended that they were unaware of and did not knowingly consent to collection of this data. According to plaintiffs, “this surreptitious use of resources had a
real cost to Plaintiffs . . . through the consumption and use of battery life, bandwidth, and file storage of their Android Mobile Phones,” and they contended that Google “potentially” exposed them to data overage charges. Plaintiffs also alleged that they paid more for their Android Mobile Phones than they would have paid if they had known Google tracked and shared their personal data. Based on these and other allegations, plaintiffs brought claims for violations of the CFAA 18 U.S.C. Section 1030 and violations of California’s Unfair Competition Law, California Business and Professions Code sections 17200, et seq. (UCL).

The CFAA Claim

Plaintiffs asserted that Google violated the CFAA. In order to bring a civil action under the CFAA, plaintiffs must be able to show a damage or loss “to 1 or more persons during any 1–year period . . . aggregating at least $5,000 in value.” Google argued that plaintiffs’ allegations were insufficient to show the requisite damage or loss. Plaintiffs relied on the allegations regarding diminished battery life, and they claimed they have sufficiently alleged damage and loss, because their service was interrupted as a result of Google’s conduct. Plaintiffs contended these allegations distinguish this case from In re iPhone App. Litig., 844 F.Supp.2d 1040 (N.D.Cal.2012). In that case, “the court found that plaintiffs had not included facts to suggest the defendant’s conduct ‘impaired’ their devices or interrupted service and, thus, failed to show damage or loss under the CFAA.” Here, plaintiffs did allege that Google’s conduct interrupted their service. Nonetheless, the Court found the allegations insufficient to state a CFAA claim:

That fact might be sufficient to satisfy the definition of “damage” set forth in 18 U.S.C. section 1030(e)(8). However, in order to pursue a civil action under the CFAA, Plaintiffs also must show economic damage or loss in the amount $5,000. 18 U.S.C. § 1030(c)(4)(A)(i)(I). Plaintiffs allege that a new battery could cost $70.00. However, none of the Plaintiffs allege that they purchased new batteries because of Google’s conduct. (See, e.g., SACC ¶¶ 98–102.) The Court concludes that the allegations regarding diminished battery life still are insufficient to allege that the economic damage or loss—even if aggregated—would reach the $5,000 threshold required by the CFAA.

Finally, Plaintiffs rely on allegations that they paid for their data plans, and that Google “used or allowed the use of a finite amount of” their data plans. Again, none of the named Plaintiffs alleged that they incurred any overage charges. Rather, they only allege that they were “potentially” exposed to overage charges. The Court concludes that the allegations regarding “loss” based on “Data Plan Utilization” are insufficient to allege that the economic damage or loss—even if aggregated—would reach the $5,000 threshold required by the CFAA. See, e.g., iPhone App. Litig. II, 844 F.Supp.2d at 1067.
Accordingly, the Court granted Google’s motion to dismiss the CFAA Claim. As “[t]his is Plaintiffs’ third iteration of the complaint,” the Court “conclude[d] that any further attempts to amend this claim would be futile.”

The UCL Claim

Plaintiff’s second claim for relief was a claim under the UCL, which prohibits “three varieties of unfair competition: practices which are unlawful, unfair or fraudulent.” The UCL also “requires that a plaintiff have ‘lost money or property’” to have standing to sue. Plaintiffs asserted that the Google’s conduct violated the fraudulent prong of the UCL. “To state a cause of action under the fraudulent prong of Section 17200, it is necessary only to show members of the public are likely to be deceived.” Allegations that the fraudulent deception was “actually false, known to be false by the perpetrator and reasonably relied upon by a victim who incurs damages” are not necessary.

Plaintiffs’ allegations were similar to the allegations in *iPhone App. Litig. II*. As the Court explained:

Specifically, Plaintiffs contend that Google’s representations that users can opt-in to location monitoring is false, because Google continues to track and store information even when the location services feature is turned off. *Cf. iPhone App. Litig. II*, 844 F.Supp.2d at 1074.

In addition, the plaintiffs allege that contrary to the representations in Google’s privacy policy, Google designed the AOS “to enable and promote the taking of Plaintiffs ... personal information so as to further monetize, for [Google’s] benefit, the advertising potential of AOSbased devices and to advance Google’s revenue model in the wireless/mobile marketplace.” (SACC ¶ 3; *see also id.* ¶ 4 (alleging that Google collected and transmitted PII “for purposes wholly unrelated to the use and functionality of” an Android mobile device or App). These allegations are similar to the allegations made by the “iDevice Class” in *iPhone App. Litig. II*. *See* 844 F.Supp.2d at 1074.

The Court concluded that these allegations, in combination with the allegations that plaintiffs relied on these statements and paid more for their mobile devices than they otherwise would have were “sufficient to *allege* a claim under the fraudulent prong.”

Google also moved to dismiss plaintiffs’ claim for restitution under the UCL on the basis that, because plaintiffs did not pay any money to Google, they are asking for “non-restitutionary disgorgement,” which is not an available remedy under the UCL. Although plaintiffs did not allege facts that show they paid money directly to Google,

the Court cannot conclude that Plaintiffs might not be able to show an ownership interest in at least some of Google’s profits. *Cf. Colgan v. Leatherman Tool Group, Inc.*, 135 Cal.App. 4th 663, 699 (2006) (a plaintiff can seek money or property as restitution where such “money or property identified as belonging
Accordingly, the Court denied, in part, Google’s motion to dismiss.

*   *   *

PRIVACY AGREEMENTS; USER AGREEMENTS; STANDING; DAMAGES; STATE NOTIFICATION LAWS

_In re Sony Gaming Networks and Customer Data Security Breach Litigation, MDL No. 11md2258 AJB (MDD) (S.D. Cal. Jan 21, 2014)_

**Sony PlayStation Data Breach Lawsuit Whittled Down but Moves Forward**

Sony’s PlayStation networks suffered a “criminal intrusion”, in the wake of which numerous users filed putative class actions. These claims were all consolidated into a single lawsuit in the Southern District of California. The judge overseeing these claims did not think highly of them, and initially dismissed them. Plaintiffs were given a chance to amend their claims, and the court issues a ruling getting rid of a majority of claims. Nevertheless, the court allowed claims based on Sony’s marketing representations that it would take reasonable steps to secure plaintiffs’ personal information and use industry-standard encryption to prevent unauthorized access to sensitive financial information.

The latest order is a 97-page behemoth that contains a comprehensive review of the various state law claims and doctrines relevant to resolving a major data breach incident. It’s almost a mini-treatise of applicable law in the area.

**Standing:** Sony argued in passing that the claims should be dismissed for failure to satisfy Article III standing, but the court rejects this argument, as it had previously. Plaintiffs had alleged that their information was acquired and wrongfully disseminated, and the court says this is sufficient for standing purposes. While Sony tried to argue that a recent Supreme Court case (_Clapper v. Amnesty International_) tightened Article III standing requirements, the court disagrees. The court says, citing to Krottner and Clapper, that plaintiffs satisfy Article III standing requirements.

**Negligence claims:** Plaintiffs asserted negligence claims based on the laws of California, Florida, Massachusetts, Missouri, and Ohio. Each claim required a showing of (1) duty, (2) breach, (3) causation, and (4) harm. The Florida, Missouri, and Ohio claims are dismissed (with prejudice) for failure to allege harm or injury. The California and Massachusetts negligence claims were based on a failure to timely notify affected persons of the breach as well as a failure to provide adequate network security. The court rejects the failure to
timely notify argument on the basis that any injury is too speculative. The court discusses the network security claim in some detail. The court says that Sony does have a legal duty to provide adequate network security, given that it is being entrusted with consumers’ confidential information. However, as to this claim, the court says that the economic loss doctrine bars recovery of purely economic damages. Plaintiffs have to allege a “special relationship” in order to escape application of the economic loss rule, and they fail to do so.

**Negligent misrepresentation/ommission:** The consolidated case involved claims for negligent misrepresentation/omission from the laws of various states (Florida, Massachusetts, Michigan, New Hampshire, Ohio, Texas, Missouri). With respect to the Ohio and Missouri claims, the court says that these are only available where the negligent misrepresentation is made for the guidance of others in the course of a business transaction. That is not the case here. As to the remaining misrepresentation claims, the court says that while the plaintiffs may have identified misrepresentations, the plaintiffs fail to allege how these misrepresentations were “reiterated and disseminated by the officers, agents, representatives . . . or employees of Defendants acting within their scope of authority.” The court also says that plaintiffs fail to adequately allege any pecuniary loss flowing from these torts. The personal information of plaintiffs does not have independent monetary value, and access to Sony’s online network was provided free. Plaintiffs argued that they would not have purchased the consoles “but for” their reliance on Sony’s misrepresentations, but because the alleged misrepresentations were contained in the PSN user agreement or privacy policy and these were presented after the purchase of the consoles, they could not have relied on these.

**Breach of warranty claims:** Plaintiffs asserted warranty claims under a variety of state laws, but not including a claim under California law. After conducting an extensive choice-of-law analysis, the court concludes that the operative user agreements require any warranty claims to be brought under California law. Because plaintiffs failed to do this, the court dismisses all of the warranty claims.

**Implied warranty claims:** Plaintiffs asserted common law and statutory warranty claims under the laws of Florida, Michigan, Missouri, New York, Massachusetts, New Hampshire, and Texas. The court says that these claims fail because: (1) the existence of a written agreement covering the warranties at issue precludes an implied warranty claim, (2) network services are not “goods” within the meaning of the UCC, and (3) most importantly, the operative user agreements contain clear and conspicuous language disclaiming any implied warranties.
Unjust enrichment claims: The court dismisses the unjust enrichment claim on the basis that plaintiffs have pled breach of contract claims and thus cannot assert unjust enrichment claims over the same subject matter.

Consumer protection claims: Plaintiffs asserted a variety of consumer protection claims, including under the laws of California, Florida, Michigan, Missouri, New Hampshire, New York, Ohio, Texas. As to the California Unfair Competition Law and Consumer Legal Remedies Act claims, the court says that plaintiffs adequately allege standing and plausibly allege fraud-based misrepresentation and omission claims. The court grants Sony’s motion as to plaintiffs Florida and Michigan unfair trade practices claim for damages but denies it as to injunctive relief. The court denies Sony’s motion as to the Missouri unfair trade practices claim. The court also denies Sony’s motion as to the New Hampshire consumer protection act claims but says that plaintiffs failed to adequately allege damages and are only entitled to injunctive relief. The New York unfair trade practices claim is dismissed due to failure to allege injury. The Ohio claims are dismissed in their entirety. Finally, the court also dismisses the Texas deceptive practices claim for failure to allege “actual injury stemming from the purchase of their Consoles and/or registration for Sony Online Services.”

California’s Database Breach Act: Claims for damages under this statute are dismissed, but claims for injunctive relief go forward.

Fair Credit Reporting Act: The court grants Sony’s motion to dismiss these claims on the basis that Sony is not a “consumer reporting agency” as defined by the statute.

February 10th Amending Order: The court issued an order on February 10th clarifying and amending the previous order as to the claims under California’s unfair competition and false advertising laws. The court clarified that it dismissed the claims for injunctive relief without leave to amend, but that claims for restitution could go forward to the extent they are premised on defendants’ alleged omissions. (The claims for restitution based on misrepresentations were dismissed.)

Absent a big change to the ground rules, Article III standing may not be the most effective way to screen out data breach lawsuits. Courts often pick between Article III and the merits, but recent cases tend to indicate the limitations of Article III in screening out these claims.

Data breach notification statutes ostensibly serve a variety of purposes, but they will probably not be useful for plaintiffs who bring damage claims. Granted, in this case, plaintiffs received notification within ten or eleven days of the breach, but the court took a fairly
restrictive view of what type of damage would satisfy causation requirements from any delayed notification.

There were several different terms of service and privacy policy provisions that consumers encountered in the course of buying products or services from Sony. The interplay between these various policies adds some factual complexity to the case. Interestingly, many of Sony’s contractual disclaimers were effective, but only after the judge scrutinized several aspects (e.g., placement, prominence) carefully.

Eventually, what ends up giving plaintiffs the best hook are Sony’s marketing representations that it would take:

reasonable steps to secure [Plaintiffs’] personal information . . . use industry-standard encryption to prevent unauthorized access to sensitive financial information.

We’ve seen this happen time and time again (e.g., Twitter’s flowery language that the FTC latched on to), and perhaps it’s an unavoidable battle between the marketing department and the legal department, but it’s worth noting that a big part of the claims that survive here is based on flowery marketing language contained in Sony’s user agreement and privacy policy. Even though there were disclaimers and limitations in the policy and notwithstanding the well-accepted notion that no one reads these policies, the court still allows claims to survive based on this language.

Given that there are no statutory damages available (restitution in the form of a refund may serve as a nice substitute), and given that the bulk of the surviving claims are types of misrepresentation-based claims that may not hold up to the light of discovery, it will be interesting to see whether the ruling prompts a settlement or whether Sony will take the route Apple took and litigate the claims.

* * *

THEFT OF PERSONAL INFORMATION; STANDING TO SUE

_In re Science Applications International_, No. 1:12-mx-00347 (D.D.C. May 9, 2014)

District Court Partially Dismisses Data Breach Case Because Plaintiffs Did Not Allege Actual or Impending Misuse or Viewing of Personal Data

In a case where a thief broke into a car containing backup tapes of personal information, Judge Boasburg held that all but two of the claims lacked standing because mere loss of data without allegations of impending misuse or viewing did not confer standing under _Clapper v. Amnesty International_. The court stressed that the facts surrounding the breach
suggested an amateur thief broke into a car for other purposes, found tapes that were difficult to decipher and did not sell the personal information on them to identity thieves. There were only two instances where the court found a plausible connection between the theft and resulting damage and therefore survived a motion to dismiss.

Because of the court’s careful and extensive analysis of the facts and law we have quoted extensively from the opinion below (citations to pleadings and some cases omitted):

This case presents thorny standing issues regarding when, exactly, the loss or theft of something as abstract as data becomes a concrete injury. That is, when is a consumer actually harmed by a data breach—the moment data is lost or stolen, or only after the data has been accessed or used by a third party? As the issue has percolated through various courts, most have agreed that the mere loss of data—without evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing. This Court agrees. Mere loss of the data is all that most Plaintiffs allege here, so the majority must be dismissed from this case.

I. Background

A. Factual Background

The tapes were backup copies of medical data related to over 4 million TRICARE beneficiaries who had received medical treatment or testing in San Antonio, Texas. … In November, SAIC mailed letters to affected service members explaining the scope of the theft and noting that “the information contained on the tapes may include names, Social Security Numbers, addresses, dates of birth, phone numbers,” and a variety of medical information. But the tapes did not include “any financial data, such as credit card or bank account information.” SAIC nevertheless offered all affected parties free credit monitoring and identity-theft protection and restoration services for one year.

Still, Plaintiffs claim that the data breach caused them substantial harm. Twenty-four of the thirty-three Plaintiffs here allege that they have been injured because of the disclosure alone. They claim that, even if no one has yet used their personal information, they face an increased risk of identity theft, which they view as a distinct and palpable harm. They also claim that the data breach violated their expectation of privacy, as codified in various statutes, state tort law, and possibly through contract. In addition, five of those twenty-four Plaintiffs claim that they have spent time or money monitoring their credit or interfacing with their banks since the theft, and that their time and effort should be compensable.

Six Plaintiffs also claim that someone used their credit cards or bank accounts without their authorization, although no one alleges that financial information was actually on the stolen tapes. One of those six additionally claims that loans have been opened in his name using his personal information—presumably including his social security number, name, date of birth, and address, all of which were on the backup tapes. Yet another Plaintiff alleges that she was harmed because her medical identity has
disappeared. Finally, two Plaintiffs allege that they have received unwanted phone calls or “phishing” emails, and one of those Plaintiffs claims that marketers have information about her medical condition that they likely obtained from the tapes.

Plaintiffs filed this lawsuit against TRICARE, which is a government agency that provides insurance coverage and health care to active-duty service members and their families and against the Department of Defense and its Secretary. The breach victims are also suing SAIC, a security firm that contracts with TRICARE to ensure the security of the personally identifiable information (PII) and protected health information (PHI) in its records.

In their Consolidated Amended Complaint, Plaintiffs allege no fewer than twenty separate causes of action, ranging from the violation of various federal statutes—such as the Privacy Act, the Fair Credit Reporting Act, and the Administrative Procedure Act—to the contravention of state statutes and common law—such as claims of negligence, breach of contract, and violation of various state consumer-protection laws. The injuries alleged include: (i) increased risk of identity theft, which Plaintiffs peg at 9.5 times their pre-theft risk; (ii) expenses incurred in mitigating the risk of identity theft; (iii) loss of privacy through the exposure of their personal information; (iv) loss of the value of their personal and medical information; (v) loss of the value of their insurance premiums, which should have been used to pay for proper security measures; (vi) SAIC’s failure to meet the requisite standard for data security; (vii) the lost right to truthful information about their data security; (viii) statutory (or liquidated) damages; and, in at least one case, (ix) actual identity theft. The Court will address each theory of injury in turn as it analyzes the standing of Plaintiffs to proceed.

III. Analysis

A. Injury in Fact

The Court will examine each element of standing in turn, beginning with injury in fact. An injury in fact is “an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” Lujan, 504 U.S. at 560 (citations and internal quotation marks omitted). “Allegations of possible future injury do not satisfy the requirements of Art. III. A threatened injury must be certainly impending to constitute injury in fact.” Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (internal quotation marks omitted) (emphasis added).

The Supreme Court recently reviewed the contours of this requirement in Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013). There, plaintiffs—who were attorneys and human-rights, labor, legal, and media organizations who worked with foreign clients or sources—contended that they were likely to be targeted for surveillance under the Foreign Intelligence Surveillance Act. See id. at 1145-46. This, they claimed, would work them harm. As such, they had taken steps to keep conversations with their clients confidential at their own personal expense. See id. The Court held, however, that plaintiffs did not have an injury in fact because the threat of surveillance was too speculative. There were, the Court reasoned,
simply too many “ifs” involved before an injury came to pass. The plaintiffs would be impacted by FISA only if (1) the government decided to target communications involving their clients and (2) used the challenged FISA provision to do so, (3) the Foreign Intelligence Surveillance Court authorized the eavesdropping, (4) the government succeeded in picking up their targets’ phone calls or e-mails, and, finally, (5) the plaintiffs were involved in whatever communication the government intercepted. *Id.* at 1147-48. The Court concluded that such “a highly attenuated chain of possibilities[] does not satisfy the requirement that threatened injury must be certainly impending.” *Id.* at 1148; see also *Whitmore*, 495 U.S. at 156-57 (speculative to assume that petitioner would request federal habeas review; habeas would be granted; petitioner would be retried for his capital offense; and thus, on appeal from this new trial, petitioner would suffer due to a lack of data on similarly situated criminal defendants); *O’Shea v. Littleton*, 414 U.S. 488, 496-97 (1974) (injury speculative where plaintiff would need to violate the law, be arrested, and be tried before a specific magistrate judge to be harmed by the judge’s allegedly illegal courtroom practice); *Los Angeles v. Lyons*, 461 U.S. 95, 105-09 (1983) (injury conjectural or hypothetical where plaintiff would have to commit an illegal act, be arrested, and be subjected to a chokehold in the future for injury to occur).

The Court added, “Respondents’ contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm” was also “unavailing—because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper*, 133 S. Ct. at 1151.

With those precepts in mind—that an injury must be present or certainly impending, that an attenuated chain of possibilities does not confer standing, and that plaintiffs cannot create standing by taking steps to avoid an otherwise speculative harm—the Court turns to Plaintiffs’ allegations of injury here.

1. **Increased Risk of Harm and Monitoring Costs**

   Plaintiffs begin by asserting that an increased risk of harm alone constitutes an injury sufficient to confer standing to sue. Due to the data breach, they claim that they are 9.5 times more likely than the average person to become victims of identity theft. That increased risk, they maintain, in and of itself confers standing. But as *Clapper* makes clear, that is not true. The degree by which the risk of harm has increased is irrelevant—instead, the question is whether the harm is certainly impending. See also *Public Citizen, Inc. v. Nat’l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1297-98 (D.C. Cir. 2007) (“‘increased risk’ is” not by “itself [a] concrete, particularized, and *actual* injury for standing purposes”—harm must be “actual” or “imminent,” not merely “increased”).

   Here, the relevant harm alleged is identity theft. A handful of Plaintiffs claims that they have suffered actual identity theft, and those Plaintiffs have clearly suffered an injury. At least twenty-four, however, allege only a *risk* of identity theft. *See supra* n.3. At this point, the likelihood that any individual Plaintiff
will suffer harm remains entirely speculative. For identity theft to occur, after all, the following chain of events would have to transpire: First, the thief would have to recognize the tapes for what they were, instead of merely a minor addition to the GPS and stereo haul. Data tapes, after all, are not something an average computer user often encounters. The reader, for example, may not even be aware that some companies still use tapes— as opposed to hard drives, servers, or even CDs—to back up their data. See Disk or Tape Backup: Which is Best?, Backup For Servers, http://goo.gl/7JsXQF (last visited Apr. 28, 2014). Then, the criminal would have to find a tape reader and attach it to her computer. Next, she would need to acquire software to upload the data from the tapes onto a computer—otherwise, tapes have to be slowly spooled through like cassettes for data to be read. Id. After that, portions of the data that are encrypted would have to be deciphered. Once the data was fully unencrypted, the crook would need to acquire a familiarity with TRICARE’s database format, which might require another round of special software. Finally, the larcenist would have to either misuse a particular Plaintiff’s name and social security number (out of 4.7 million TRICARE customers) or sell that Plaintiff’s data to a willing buyer who would then abuse it.

The vast majority of Plaintiffs has not alleged that any of those things have happened—because they cannot. Those events are entirely dependent on the actions of an unknown third party—namely, the thief. At this point, we do not know who she was, how much she knows about computers, or what she has done with the tapes. The tapes could be uploaded onto her computer and fully deciphered, or they could be lying in a landfill somewhere in Texas because she trashed them after achieving her main goal of boosting the car stereo and GPS. Unfortunately, there is simply no way to know until either the crook is apprehended or the data is actually used. Courts for this reason are reluctant to grant standing where the alleged future injury depends on the actions of an independent third party. See Clapper, 133 S. Ct. at 1150 (expressing “our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors”).

That is, no doubt, cold comfort to the millions of servicemen and women who must wait and watch their credit reports until something untoward occurs. After all, it is reasonable to fear the worst in the wake of such a theft, and it is understandably frustrating to know that the safety of your most personal information could be in danger. The Supreme Court, however, has held that an “objectively reasonable likelihood” of harm is not enough to create standing, even if it is enough to engender some anxiety. See id., 133 S. Ct. at 1147-48. Plaintiffs thus do not have standing based on risk alone, even if their fears are rational.

Nor is the cost involved in preventing future harm enough to confer standing, even when such efforts are sensible. See id. at 1150-51. There is, after all, nothing unreasonable about monitoring your credit after a data breach. In fact, that is exactly what TRICARE and SAIC advised Plaintiffs to do—and what SAIC, in part, offered to pay for. See, e.g., Letter from SAIC at 1. But the Supreme Court has determined that proactive measures based on “fears of… future harm that is not certainly impending” do not create an
injury in fact, even where such fears are not unfounded. *Clapper*, 133 S. Ct. at 1151. Put another way, the Court has held that plaintiffs cannot create standing by “inflicting harm on themselves” to ward off an otherwise speculative injury. *Id.* The cost of credit monitoring and other preventive measures, therefore, cannot create standing.

There is, however, an alternative argument. Plaintiffs point out that, in *Clapper*, the Court acknowledged that it sometimes “found standing based on a ‘substantial risk’ that… harm will occur, which [could] prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.” *Clapper*, 133 S. Ct. at 1150 n.5 (emphasis added). So Plaintiffs could, theoretically, prevail if the risk of harm here were substantial. Yet, Plaintiffs’ Complaint itself makes clear that they do not surmount that hurdle. To be sure, Plaintiffs allege that data-breach victims in general are 9.5 times more likely than the average person to experience identity theft post-breach. But then Plaintiffs note that, overall, only about 19% of breach victims actually experience identity theft. *Id.* By Plaintiff’s own calculations, then, injury is likely not impending for over 80% of victims—and the figure is likely to be considerably higher in this case, where the theft was unsophisticated and where the lack of widespread harm suggests that the tapes have not ever been accessed. Cf. *Galaria*, 2014 WL 689703, at *5. The harm in these circumstances, therefore, cannot satisfy the requirement of either the Supreme Court or the D.C. Circuit that there be “(i) a substantially increased risk of harm and (ii) a substantial probability of harm with that increase taken into account.” *Public Citizen, Inc.*, 489 F.3d at 1295. . . .

Litigants’ cost-of-monitoring claims fared no better. See, e.g., *Reilly*, 664 F.3d at 46 (“Appellants’ alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more ‘actual’ injuries than the alleged ‘increased risk of injury’ which forms the basis for Appellants’ claims.”); *Randolph*, 486 F. Supp. 2d at 8 (The “argument that the time and money spent monitoring a plaintiff’s credit suffices to establish an injury overlook[s] the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized.”) (internal quotation marks omitted).

This is not to say that courts have uniformly denied standing in data-breach cases. See, e.g., *Holmes v. Countrywide Fin. Corp.*, No. 08-205, 2012 WL 2873892, at *5-*11 (W.D. Ky. July 12, 2012); *McLoughlin v. People’s United Bank, Inc.*, No. 08-944, 2009 WL 2843269, at *3-*4 (D. Conn. Aug. 31, 2009); *Doe 1 v. AOL*, 719 F. Supp. 2d 1102, 1109 (N.D. Cal. 2010); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 279-80 (S.D.N.Y. 2008). Most cases that found standing in similar circumstances, however, were decided pre-*Clapper* or rely on pre-*Clapper* precedent and are, at best, thinly reasoned. For example, in *Ruiz v. Gap, Inc.*, 380 Fed. Appx. 689 (9th Cir. 2010) (Gap III), the court stated that a “credible threat of harm is sufficient to constitute actual injury for standing purposes.” *Id.* at 691; see also, e.g., *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010) (“the possibility of future injury may be sufficient to confer standing on plaintiffs; threatened injury constitutes ‘injury in fact’”)

96
(quoting *Cent. Delta Water Agency v. United States*, 306 F.3d 938, 947 (9th Cir. 2002)); *Pisciotta v. Old Nat’l Bancorp*, 499 F.3d 629, 632 (7th Cir. 2007) (standing because “the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious”). Yet after *Clapper*, *Gap III’s* “credible threat of harm” standard is clearly not supportable.

Indeed, since *Clapper* was handed down last year, courts have been even more emphatic in rejecting “increased risk” as a theory of standing in data-breach cases. As one court noted, after “*Clapper*, the mere fact that the risk has been increased does not suffice to establish standing.” *Strautins v. Trustwave Holdings, Inc.*, No. 12-9115, 2014 WL 960816, at *4 (N.D. Ill. Mar. 12, 2014). After all, an *increased risk or credible threat* of impending harm is plainly different from *certainly impending* harm, and certainly impending harm is what the Constitution and *Clapper* require. *Clapper*, 133 S. Ct. at 1148; see, e.g., *Strautins*, 2014 WL 960816, at *4 (deciding in light of *Clapper* that injury was speculative based “on a number of variables, such as whether their data was actually taken during the breach, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded”); *Galaria*, 2014 WL 689703, at *5 (noting the similarity to *Clapper* and holding that “[i]n this case, an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege—or offer facts to make plausible—an allegation that such harm is ‘certainly impending’”); *Polanco v. Omnicell, Inc.*, No. 13-1417, 2013 WL 6823265, at *14 (D.N.J. Dec. 26, 2013) (relying on *Clapper* and *Reilly* to conclude that mere loss of data, without misuse, is not “an injury sufficient to confer standing”); but see *In re Sony Gaming Networks & Customer Data Sec. Breach Litigation*, MDL No. 11-2258, 2014 WL 223677, at *9 (S.D. Cal. Jan. 21, 2014) (finding standing post-*Clapper* based on a “plausibly alleged… ‘credible threat’ of impending harm”).

In sum, increased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm. At least twenty-four of the thirty-three Plaintiffs in this case, then, must rely on an alternative theory of injury.

2. Privacy

Plaintiffs also allege that they have been injured because their privacy was invaded by the data breach. Yet this claim suffers from the same defects as Plaintiffs’ previous contention. For a person’s privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party. Existing case law and legislation support that common-sense intuition: If no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated. . . .

Here, the majority of Plaintiffs contend neither that their personal information has been viewed nor that their information has been exposed in a way that would facilitate easy, imminent access. As in the Third Circuit case *Reilly*, it would be speculative to assume that the thief “read, copied, or understood the data.” 664 F.3d at 40. As a result, no invasion of Plaintiffs’ privacy is imminent.
To be sure, the Supreme Court has intimated that disclosure of personally identifiable information alone, along with some attendant emotional distress, may constitute “injury enough to open the courthouse door” in privacy actions. Doe v. Chao, 540 U.S. 614, 624-25 (2004). But again, disclosure involves publication to a third party. In that case, Doe’s social security number had actually been published by the government on various documents “sent to groups of [workers’-compensation] claimants, their employers, and the lawyers involved in their cases.” Id. at 617. In other words, Doe’s information was actually exposed to dozens of readers. Here, by contrast, disclosure and access of Plaintiffs’ personal information is anything but certain. Rather, the information itself is locked inside tapes that require some expertise to open and decipher. Indeed, it is highly unlikely that the crook even understood what the tapes were, let alone had the wherewithal to access them or navigate her way to any one of the 4.7 million records contained therein. And until Plaintiffs can aver that their records have been viewed (or certainly will be viewed), any harm to their privacy remains speculative.

A few of the Plaintiffs here do allege that their data was used. Those Plaintiffs have at least claimed an injury to their privacy insofar as they allege that their data was accessed. The other Plaintiffs, however, are out of luck.

3. Loss of Value

Plaintiffs next contend that they were injured by the loss of two valuable assets. First, they argue that they lost the value of their personal and medical information, which could be “sold on the cyber black market for $14 to $25 per medical record.” Second, they claim they forfeited the value of their insurance premiums, which should have been used to pay for better security.

As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss. Even if the service members did intend to sell their own data—something no one alleges—it is unclear whether or how the data has been devalued by the breach. For those reasons, Plaintiffs’ first theory of injury is unsuccessful.

Similarly, as to the value of their insurance premiums, Plaintiffs do not plausibly allege any actual loss. They allege that they were paying for “health and dental insurance”—and they do not claim that they were denied coverage or services in any way whatsoever. See id. To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing. They do not maintain, moreover, that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime. Put another way, Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid. Nothing in the Complaint makes a plausible case that Plaintiffs were cheated out of their premiums. As a result, no injury lies.
4. Legal Violations

Plaintiffs next set forth various legal violations that they claim create standing: They argue that SAIC failed to meet the requisite legal standards for data security; that SAIC and TRICARE violated their right to truthful information about their data; and that certain statutes, if violated, give them the right to automatic damages or payment. Standing, however, does not merely require a showing that the law has been violated, or that a statute will reward litigants in general upon showing of a violation. Rather, standing demands some form of injury—some showing that the legal violation harmed you in particular, and that you are therefore an appropriate advocate in federal court.

As the Supreme Court “has repeatedly held…[,] an asserted right to have the [defendant] act in accordance with law is not sufficient, standing alone, to confer jurisdiction on a federal court.” Allen v. Wright, 468 U.S. 737, 754 (1984). Rather, the unlawful activity must work some harm on Plaintiffs.

In terms of the alleged contravention of security standards, Plaintiffs have not outlined any actual or imminent harm caused by that purported violation—aside from the theories the Court has already rejected. Plaintiffs, therefore, cannot acquire standing on that basis.

The same is true of the supposed deprivation of Plaintiff’s “right to truthful information about the security of their PII/PHI.” Opp. to SAIC at 7. No independent harm has flowed from that so-called deprivation. Of course, as Plaintiffs point out, denial of information alone can sometimes create an injury when statutes require disclosure. See Zivotofsky ex rel. Ari Z. v. Sec’y of State, 444 F.3d 614, 617-19 (D.C. Cir. 2006) (noting that violation of plaintiff’s right to documents under Freedom of Information Act can create standing). Here, however, Plaintiffs have failed to allege any actual deprivation of information, even assuming they have a right to it. First, they claim that they were deprived of information before TRICARE and SAIC notified them of the data breach. Any injury that might have occurred during that time, however, has been cured, since SAIC has now explained the extent of the breach to Plaintiffs in some detail and no one alleges any independent harm caused by the delay. Indeed, expedient notification of the data breach and its scope, along with certain required contact information, is all the relevant laws demand. See, e.g., Cal. Civ. Code § 1798.82; Or. Rev. Stat. Ann. § 646A.604(1)-(2). In addition, Plaintiffs claim that they have been deprived of truthful information because SAIC “[c]ategoriz[ed] the risk of access” to their data “as ‘low’” in their letters notifying servicemen of the breach. But that is, at best, a difference of opinion—Plaintiffs do not identify any actual facts that SAIC or TRICARE has withheld. As a result, Plaintiffs’ abstract assertion that their “right to truthful information” has been violated does not constitute an injury, since the facts in the complaint identify neither an actual deprivation nor any independent harm.

5. Actual Misuse

As noted above, Plaintiffs who claim that their information was, in fact, accessed and misused have alleged an actual injury. That injury, however, must still be linked to Defendants’ conduct.
B. Causation


To review the bidding: The majority of Plaintiffs in this case lack standing to sue because they failed to allege any cognizable injury. Six Plaintiffs, however, claim that their data was actually misused; one Plaintiff claims she has suffered medical fraud; and two claim that their privacy was invaded by phone calls and other solicitations from companies that may have accessed their medical records. Each of these three groups of Plaintiffs must be able to link their harm to the data breach.

1. Identity Theft

Six out of thirty-three Plaintiffs allege that their personal information was used for fraudulent purposes. See supra n.5. Five of those six claim only that unauthorized charges were made to their existing credit cards or debit cards, or that money was withdrawn from an existing bank account. But here’s the problem: No one alleges that credit-card, debit-card, or bank-account information was on the stolen tapes. To be sure, as Plaintiffs’ counsel noted at the Court’s August hearing, a criminal could obtain some of a victim’s personal information from a data breach and then go “phishing” to get the rest. See Hrg. Tr. at 45-46. That is, the crook could acquire a name and phone number and then make calls pretending to be a legitimate business asking for information like credit-card or bank-account numbers. Here, however, the identity-theft Plaintiffs have not alleged any phishing. Indeed, they proffer no plausible explanation for how the thief would have acquired their banking information. In a society where around 3.3% of the population will experience some form of identity theft—regardless of the source—it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud. See Kristin Finklea, Cong. Research Serv., R40599, Identity Theft: Trends and Issues 1 (2014), available at http://goo.gl/bCsTEg (10.2 million Americans, out of around 308.7 million total, experienced identity theft in 2010). As that information was not on the tapes, though, Plaintiffs cannot causally link it to the SAIC breach.

One Plaintiff, however—Robert Curtis, a Colorado resident—may have a case. After the data breach, he received “letters in the mail from American Express,” among others, “thanking him for applying for loans” that he had never applied for. To apply for such a loan, one would likely need a person’s name, address, date of birth, and social security number—exactly the sort of information that was on the tapes. The Court believes that this creates a sufficient causal link between the identity theft—which has hurt Curtis’s credit history,— and the tape theft.

That said, the Court would be remiss if it did not note that Curtis also alleges a spate of identity theft that cannot plausibly be linked to the tapes. For example, he also complains that many of his existing
accounts have been tampered with in seriously concerning and, no doubt, frustrating ways. *Id.* In one instance, Curtis’s bank notified him when “an individual in Mexico” called his bank asking for money “and knew Plaintiff Curtis’ account number, unlisted telephone number, address, date of birth and e-mail address, Social Security number and answers to the security questions.” No one alleges, however, that the name of Curtis’s bank, his account number, his e-mail address, or the answers to his security questions were on the stolen tapes. He also claims that “individuals wired approximately $32,500 out of his credit union account.” *Id.* But again, he does not claim that the account information was on the tapes, although he does aver that he gave TRICARE his payment information at some point. *Id.* The inescapable conclusion is that Curtis has been subjected to another, more profound data breach involving his financial—not medical—records.

As a result, the fraudulent loan applications may also be linked to this other, more severe data breach and not the SAIC breach. At this point, however, the Court is willing to give Curtis the benefit of the doubt, since there is at least a plausible connection between some of the harm he has suffered and the SAIC theft.

2. *Medical Fraud*

Another Plaintiff, Robin Warner, claims that she experienced medical fraud because her medical records no longer exist. This is a striking allegation, but it cannot establish standing because only backup tapes were stolen from the SAIC employee’s car. Warner does not explain how the disappearance of her medical identity can be linked to the theft of tapes that contained only copies of her actual medical records. She has thus not carried her burden of alleging causation and hence has no standing.

3. *Privacy*

Two final Plaintiffs—in addition to Curtis, who has experienced similar woes—claim that their privacy has been invaded due to the data breach. Murray Moskowitz simply alleges that he “has received a number of unsolicited calls from telemarketers and scam artists.” He does not otherwise link the calls to the tapes, claim that the callers have personal or private information found on the tapes, or even allege that his phone number was unlisted and hence would have been difficult for marketers to locate absent the assistance of the data thief. Moskowitz seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls. His harm, consequently, cannot plausibly be linked to the tapes.

Dorothy Yarde, on the other hand, does allege a credible link to the data breach. She claims that her “telephone number is unlisted.” Still, after the theft, “she received numerous unsolicited telephone calls from insurance companies and other[s]” pitching “medical products and services… targeted at a specific medical condition listed in her medical records.” *Id.* (emphasis added). She had not received such calls in the past. *Id.* The fact that the callers had Yarde’s unlisted phone number and medical diagnosis—both of which were on the tapes—suffices to create a causal link.
C. Redressability

The third and final element of standing is redressability, which requires that it “be ‘likely,’ as opposed to merely ‘speculative,’ that the” alleged “injury will be ‘redressed by a favorable decision.’” *Lujan*, 504 U.S. at 561 (citation omitted).

At this point, only two Plaintiffs remain: Curtis, who has alleged actual misuse of his social security number, and Yarde, who has alleged a privacy violation linked to her medical information. Both harms can be redressed, at least in part, by a monetary reward. Those two Plaintiffs—and only those two Plaintiffs—therefore have standing to sue.

* * *

A reasonable reader may still wonder: If Curtis and Yarde’s information was potentially accessed or misused, why not presume that the remaining Plaintiffs’ information will suffer the same fate? Indeed, other courts have allowed cases to move forward where some form of fraud had already taken place. For example, in *Anderson v. Hannaford Bros.*, 659 F.3d 151 (1st Cir. 2011), the First Circuit declined to question the plaintiffs’ standing where 1,800 instances of credit-and debit-card fraud had already occurred and had been clearly linked to the data breach. *Id.* at 162-67. Similarly, in *Pisciotta*, the court allowed plaintiffs to proceed where “the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious;” and thus that the potential for harm was indeed substantial. 499 F.3d at 632.

The circumstances here, however, are starkly different. First, the theft from the SAIC employee’s car was a low-tech, garden-variety one. Any inference to the contrary is undermined by the snatching of the GPS and car stereo. This is hardly a black-ops caper. Second, while Curtis and Yarde have alleged personalized injury sufficient to surmount a motion to dismiss under Rule 12(b)(1), there are no facts here that plausibly point to imminent, widespread harm. In fact, the link between Curtis and Yarde’s injuries and the data breach barely crosses the line from possible to plausible. Curtis, after all, was almost certainly the victim of another, more severe data breach, and that breach may well have been responsible for every instance of identity theft he alleges. It remains likely, in other words, that no one accessed his information from the tapes. Yarde’s harm may also stem from another source. For example, she might have bought specific medications related to her condition over the counter at the neighborhood drugstore or online. That information could have been sold to companies targeting such patients—no data breach necessary. At this stage, the Court simply acknowledges that the link between the data breach and Yarde and Curtis’s claims is *plausible*, even if it is very likely that their harm stems from another source.

The fact that Curtis and Yarde’s allegations are plausible, however, does not lead to the conclusion that wide-scale disclosure and misuse of all 4.7 million TRICARE customers’ data is plausibly “certainly impending.” *Clapper*, 133 S. Ct. at 1147. After all, as previously noted, roughly 3.3% of Americans will experience identity theft of some form, regardless of the source. *See* Finklea, *Identity Theft: Trends and
Issues, supra, at 1. So one would expect 3.3% of TRICARE’s customers to experience some type of identity theft, even if the tapes were never read or misused. To quantify that percentage, of the 4.7 million customers whose data was on the tapes, one would expect around 155,100 of them to experience identity fraud simply by virtue of living in America and engaging in commerce, even if the tapes had not been lost. Here, only six Plaintiffs allege some form of identity theft, and out of those six only Curtis offers any plausible link to the tapes. And Yarde is the only other Plaintiff—out of a population of 4.7 million—who has offered any evidence that someone may have accessed her medical or personal information.

Given those numbers, it would be entirely implausible to assume that a massive identity-theft scheme is currently in progress or is certainly impending. Indeed, given that thirty-four months have elapsed, either the malefactors are extraordinarily patient or no mining of the tapes has occurred. This is simply not a case where hundreds or thousands of instances of fraud have been linked to the data breach. See, e.g., Anderson, 659 F.3d at 162-67. Rather, as far as the Court is aware, only six instances of fraud have been reported, and only two customers can plausibly link either identity theft or privacy violations to the tapes’ loss. As such, only those two Plaintiffs whose harm is plausibly linked to the breach may move forward with their claims.

IV. Conclusion

Since the majority of Plaintiffs has been dismissed—potentially altering the scope of the remaining litigants’ claims moving forward—the Court will pause to confer with the parties before determining which, if any, of the Complaint’s twenty counts has been properly alleged. The Court thus reserves the issue of whether Defendants’ Rule 12(b)(6) Motions should be granted for a future date. It further notes that it expects the parties to confer before the forthcoming status to determine if they can reach some agreement on the next procedural steps in the case.

For the aforementioned reasons, the Court will grant in part and deny in part Defendants’ Motions to Dismiss. A separate Order consistent with this Opinion will be issued this day.

*   *   *
PRIVACY/SECURITY; PUBLICITY/PRIVACY RIGHTS

In re Google Android Consumer Privacy Litigation, 1-MD-02264 JSW (N.D. Cal. Mar. 10, 2014)


Android and Pandora Privacy Rulings Accept Low Hurdle for Standing

By Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

A pair of rulings from Judge White in lawsuits involving the privacy practices of Android and Pandora employ a loose standard for standing and allowed plaintiffs in both cases to press forward with their claims.

Judge White recently rejected Google’s request to dismiss claims that Google—through the Android platform—gained access to and improperly passed to third parties (or allowed third parties to access) personal information:

- class Members’ home and workplace locations and current whereabouts;
- several universally unique device identifiers (“UUIDs”) assigned to Plaintiffs’ Android mobile phones;
- other device-specific data that was useful to Google and third parties for purposes of “device-fingerprinting;” (i.e., the creation of a back-up unique identifier to engage in tracking of a particular device);
- along with personal information about Plaintiffs such as their gender and age, what functions Plaintiffs performed on Apps, search terms entered, and selections of movies, songs, or restaurants.

Highlights of the ruling:

- the court rejects Google’s standing argument, finding that at the pleading stage, plaintiffs have sufficiently alleged standing
• the court grants Google’s request to jettison the Computer Fraud and Abuse Act claim, finding that even if plaintiffs’ damage allegations are aggregated, they fail to satisfy the damage threshold
• the court dismisses the UCL claim based on the unlawful prong since it piggybacked on the CFAA claim
• the court declines the request to dismiss the UCL claim based on the unfairness prong (“Unfair simply means any practice whose harm to the victim outweighs any benefits.”)
• the court also declines the request to dismiss the UCL claim under the fraudulent prong — here, the court cites to Google’s privacy policy and says that several of Google’s actual practices are allegedly “contrary to the representations in Google’s privacy policy”
• finally, the court also rejects Google’s argument that plaintiffs are not entitled to restitution because money wasn’t paid directly to Google

The court also cites to the recent ruling in a privacy lawsuit against Apple, which initially left some claims standing but ultimately dismissed those claims at the summary judgment stage. (See Privacy Plaintiffs Lose Because They Didn’t Rely on Apple’s Privacy Representations — In re iPhone App Litigation.)

Pandora was sued for making misrepresentations regarding its disclosure of personal information to third parties. The court initially dismissed the lawsuit in an order that made me think plaintiff would not want to re-file, but plaintiff, along with other putative class action reps, re-filed. (See “Judge Boots Privacy Lawsuit Against Pandora but Plaintiffs Can Replead – Yunker v. Pandora”.) This time around the court declines Pandora’s motion to dismiss.

Pandora’s privacy policy provides that it will:

use and share non-personally identifiable information, such as general demographic or location information, or information about the computer or device from which you access [the Pandora App]. Additionally, we may de-identify personally identifiable information and share it in a de-identified or aggregated form with third parties, advertisers and/or business partners in order to analyze [Pandora] usage, improve the Pandora Services and your listener experience, or for other similar purposes. The use and disclosure of such information is not subject to any restrictions under the Privacy Policy. [emphasis added]

Plaintiffs claimed that sharing of personal information such as age, gender, location, and the device identifier violated the privacy policy, which promised to only use such information to analyze usage, improve services, “or for other similar purposes.” Some of the plaintiffs were premium (paying) customers.
Standing: The court previously concluded that plaintiff failed to allege sufficient facts to satisfy standing but this time around, says that plaintiffs’ allegations regarding “decreased memory space” satisfies standing. The court also cites to their allegations that their PII was economically valuable and that plaintiffs would not have paid fees or turned over their PII had they known how Pandora would misuse it.

UCL Claim: The court previously dismissed the UCL claim on standing grounds, but this time around says that plaintiffs satisfy standing. The court cites again to the use of memory and additional fees incurred by plaintiffs.

Breach of contract: The court also declines to dismiss plaintiffs’ breach of contract claim. Pandora argued that the privacy policy is not an agreement but the court disagrees (without any real citations). As for damages, the court again cites to “the overage [plaintiffs’ suffered] on their data and memory plans.”

Privacy claim under the California Constitution: The court previously dismissed this claim because Pandora’s acts were not an “egregious breach of the social norms underlying the privacy right.” Plaintiffs’ amended complain doesn’t change the court’s view.

Ouch. A diluted test for standing strikes again. Both of these cases are good examples of a court applying nominal scrutiny to the allegations of a privacy plaintiff. It’s tough to mark an exact point where a shift occurred, or even know that it has, but my sense is that standing is increasingly becoming less useful for defendants in privacy cases. These cases don’t raise the issue of statutory standing, where courts have always been more permissive; at this point, these cases involved UCL and breach of contract claims.

These lawsuits may end up going the way of the first generation cookie lawsuits. The slight difference between the two is that while the previous lawsuits were based on privacy intrusions that occurred while plaintiffs were using free services, these lawsuits involve products that were nominally purchased. For this reason, the unfair competition claims are a good hook, at least at the initial stages. Further factual development may show, for example, that the plaintiffs did not rely on Google’s representations or that they haven’t been harmed in a benefit-of-the-bargain sense. This is ultimately what happened with the iPhone app litigation, and I wouldn’t be surprised if a similar outcome was in store for these plaintiffs. [It’s unclear as to the precise extent to which the Pandora plaintiffs’ status as paying customers affects their overall chances. Only some of the plaintiffs are paying customers, but the court doesn’t specify whether the chances of recovery are different for paying versus non-paying customers.]
The Pandora ruling in particular is a good lesson on the privacy policy drafting front. Companies are reluctant to come out and say that they will use personal information for “marketing purposes,” but that’s what Pandora should have done here. Granted, their privacy policy is equivocal, and there is arguably helpful language that use of “de-identified personally identifiable information . . . is not subject to any restrictions” under the policy, but this conflicts with the policy’s listing of the types of uses for de-identified information. There is always some tension between various stakeholders, but a good line to draw would be to assure customers that you would not use their personal information for “direct marketing” (perhaps defined as marketing via email, telephone, postal mail and other similar means), but you would use it for other types of marketing. Or perhaps that you would use demographic information for marketing. It’s also worth noting that both the court’s ruling and the policy as interpreted by the court use a broad (or ambiguous) definition of PII. (Cf. “California Supreme Court Rules That a ZIP Code is Personal Identification Information — Pineda v. Williams-Sonoma“.)

As a final note, I wouldn’t be surprised if the allegations regarding the collection and transmission of information by Google and app-developers have some shred of truth to them. These lawsuits are typically fashioned around the findings of security/privacy researchers that have some measure of reliability. Of course, that doesn’t mean that it was a conscious decision by Google, or even that there’s a direct financial benefit as a result of the collection and disclosure of information in question. Still, it’s a sad state of affairs when the biggest mobile platforms are facing allegations that their privacy practices turned out to not be as promised.

Related posts:

Privacy Plaintiffs Lose Because They Didn’t Rely on Apple’s Privacy Representations — In re iPhone App Litigation

Class Action Against Path Over Cellphone Address Book Access Keeps Going

Judge Koh Whittles Down iPhone App Privacy Lawsuit

Google Wins Cookie Privacy Lawsuit

Flash Cookies Lawsuit Tossed for Lack of Harm—La Court v. Specific Media

Judge Recognizes Loss of Value to PII as Basis of Standing for Data Breach Plaintiff — Claridge v. RockYou

Another Lawsuit over Flash Cookies Fails — Bose v. Interclick
CONTENT REGULATION. SPAM

* * *


Yahoo! Scores Significant Win in Email-to-SMS Lawsuit

By Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

We’ve blogged a bunch about text spam lawsuits in general, and about those against Yahoo! as well. Most recently, a judge denied Yahoo!’s request to dismiss a lawsuit relating to IM-to-SMS functionality. (See “TCPA Claim Over Yahoo!’s IM to SMS Messaging Survives Summary Judgment.”)

In contrast to the result in the California case, in federal court in Pennsylvania, Yahoo! prevailed in a putative class action alleging that its email-to-SMS functionality violated the TCPA.

Plaintiff alleged that he obtained a cell phone and number and that the previous owner of the number had enrolled in Yahoo!’s email-to-SMS functionality. That is, plaintiff alleged that he never signed up to receive any text messages from Yahoo! but nevertheless received them.

Plaintiff filed a lawsuit in April 2013. Yahoo! quickly moved for summary judgment on the basis that Yahoo! did not use an “autodialer” as required by the statute and case law.

The statute covers unsolicited texts sent using equipment which has the capacity to store or produce numbers “using a random or sequential number generator” and to dial such numbers. The Ninth Circuit in Satterfield v. Simon & Schuster articulated a watered down standard for this requirement: “a system need not only store, produce, or call
randomly or sequentially generated telephone numbers, it need only have the capacity to do so.” (See this post for a discussion of Satterfield.)

After limited discovery, the court grants Yahoo!’s motion and dismisses the lawsuit. The court relies on a declaration from a product manager from Yahoo! to the effect that the equipment used by Yahoo! “[does] not have the capacity to store or produce telephone numbers to be called, using a random or sequential number generator, and to call those numbers.” Plaintiff tried to contest the product manager’s declaration and offer his own expert testimony, but the court is not persuaded. Although unclear, the court seems to say that the “system” can generate random numbers and then text those numbers, but can only perform both of those functions if it has some software installed. At any rate, the court does not say that it’s using a standard that’s different from the one in Satterfield, but seems to imply that the requirement to generate random numbers and then dial (or text) them is conjunctive, rather than disjunctive (i.e., the equipment has to have the ability to generate numbers and call those numbers that are generated). Interestingly, the court focuses on the fact that the equipment alone does not have that capacity, but with the installation of software it would easily obtain it.

This is a BIG win for Yahoo! Make no mistake about it. Since it’s a district court opinion, it will have limited effect, until affirmed, but how to explain this:

- Yahoo! engaged in procedural jockeying that turned out to be advantageous (filing an early summary judgment motion)
- the trial court parsed Satterfield and employed a slightly different definition
- Yahoo!’s engineer did a nice job articulating minor differences between the capacity of the equipment and what was required by the statute
- the trial court recognized this lawsuit for what it was – a bogus attempt to capitalize on an overly broad statute

Either way, the problem of recycled phone numbers is not a very easy one to solve, but perhaps Yahoo! or the phone companies will put some energy into trying to come up with some fixes. (Cf. Telephone Numbers as Identity Authenticators—Abrams v. Facebook.) In the meantime, this lawsuit will likely be consigned to the dustbin, where it belongs.

Related posts:

TCPA Claim Over Yahoo!’s IM to SMS Messaging Survives Summary Judgment
Confirmatory Opt-out Text Message Not Actionable Under the TCPA — Ryabyshchuck v. Citibank
Confirmatory Opt-Out Text Message Doesn’t Violate TCPA – Ibey v. Taco Bell

Court Affirms Robust ISP Protection For Blocking Bulk Emails — Holomaxx v. Microsoft/ Yahoo

Telephone Numbers as Identity Authenticators–Abrams v. Facebook

Group Text Services Grapple with TCPA Class Actions

Courts Allows Text Spam Class Action Against Voxer, a Cell Phone Walkie-Talkie App — Hickey v. Voxernet

Ninth Circuit Revives TCPA Claim—Satterfield v. Simon & Schuster

Cellphone Spam Violates TCPA–Joffe v. Acacia Mortgage

Text Spam Lawsuit Against Citibank Moves Forward Despite Vague Allegations of Consent — Ryabyshchuk v. Citibank

Court Rejects Constitutional Challenge to TCPA Based on Vagueness in “Prior Express Consent” Exception — Kramer v. Autobytel, Inc.

Another Court Finds that TCPA Applies to Text Messages — Lozano v. Twentieth Century Fox Film Corp.

Court Finds that SMS Spam Messages are Subject to the TCPA and Rejects First Amendment Defense — Abbas v. Selling Source, LLC

Franchisor Isn’t Liable Under the TCPA for Franchisees’ Text Message Campaign – Thomas v. Taco Bell

* * *

MARKETING


(March 25, 2014)

Supreme Court Changes False Advertising Law Across the Country

By Eric Goldman

http://www.blog.ericgoldman.org

Last week, in *Lexmark v. Static Control*, the Supreme Court articulated new standards about who can sue for false advertising under federal law. Because the Supreme Court rejected all of the disparate legal tests currently being used, this ruling will change false
advertising law across the country. While it’s not clear who will win and lose from the new rule, it is clear that everyone should benefit from a uniform national rule about who can sue for what.

The Court’s Holding

The Lexmark lawsuit involves a manufacturer’s allegedly false statements about a supplier of components to rival manufacturers. The manufacturer/defendant was not a “direct” competitor of the component manufacturer/plaintiff; but undoubtedly the manufacturer’s statements were likely to suppress demand for the component manufacturer’s product. The component manufacturer claimed that the manufacturer’s disparaging remarks constituted false advertising under the Lanham Act. I explain the lawsuit’s history more in my Supreme Court preview.

The Lanham Act implies, but doesn’t directly say, that not everyone has the right to sue (what’s called “standing”) for violations; instead, it requires some sort of competitive injury. Due to the ambiguities of the statutory language, appellate courts throughout the country had adopted a variety of tests to decide who had standing for a Lanham Act false advertising claim. One test limited standing only to direct competitors of the defendant; other tests permitted a broader range of interested plaintiffs.

In the Lexmark opinion, authored by Justice Scalia, the Supreme Court rejected all of the appellate courts’ existing tests, as well as other tests favored by the litigants and their amici. Instead, the Supreme Court crafted a completely new standing rule requiring that the plaintiff be within the statute’s “zone of interest” and the plaintiff’s injuries be “proximately caused” by the false representation. Thus, Lanham Act false advertising standing requires the plaintiff to allege:

an injury to a commercial interest in reputation or sales…flowing directly from the deception wrought by the defendant’s advertising; and that that occurs when deception of consumers causes them to withhold trade from the plaintiff.

Implications

In some jurisdictions, such as those that limited standing to direct competitors, the Supreme Court’s ruling will probably expand the number of potential plaintiffs over a business’ false assertions. For example, the ruling provides standing for a component supplier if a manufacturer of finished goods bashes the component, even if the parties aren’t direct competitors. The opinion also might mean that a retailer can sue manufacturer A for bashing manufacturer B if the bashing cuts into the retailer’s sales.
However, in jurisdictions that had adopted broader standing tests, this ruling might reduce the number of potential false advertising plaintiffs. Furthermore, the opinion indicates that some plaintiffs categorically lack standing, including consumers, businesses buying for their own account, and service providers to a business harmed by a false representation, such as landlords or power companies. These categorical exclusions aren’t a big change to existing law, but they ensure that Lanham Act false advertising won’t evolve into a general-purpose false advertising law.

The court’s requirement of a proximately caused injury might further restrict who can sue. It won’t be enough for a business to simply point to someone else’s commercial statement, claim it’s false, and run to the courthouse. We’ll have to see how rigorously lower courts interpret this “injury” requirement, but it could lead to further reductions in the number of plaintiffs with standing.

Thus, although the Supreme Court rejected the narrowest standing test and said that standing was possible in this case, the Supreme Court’s holding may, on balance, lead to a net reduction in the universe of plaintiffs with Lanham Act false advertising standing.

Either way, this ruling should eliminate the different regional tests for standing. Instead, it establishes a common legal standard across the nation. That reduces the risks of litigation gamesmanship in deciding where to sue, and it should reduce the litigation costs to determine standing. It helps that this ruling was a single unanimous opinion—a truly remarkable outcome given that the court adopted a test advocated by none of the litigants, and further remarkable because Justice Alito wrote one of the appellate court opinions that this opinion effectively overturns.

It’s worth reiterating that the question resolved in Lexmark v. Static Controls was narrow: standing for Lanham Act false advertising. Other overlapping false advertising laws are not affected. So even if this ruling means a plaintiff now can’t bring a false advertising claim under the Lanham Act, the plaintiff still may have recourse under a myriad of other legal doctrines.

The Supreme Court has a second false advertising case, POM Wonderful v. Coca-Cola, still pending on its docket. I plan to preview that case in a couple weeks. The Supreme Court rarely takes false advertising cases, so having two in one year is a big deal for the advertising law community.

*   *   *

112
LICENSING/ CONTRACTS, PUBLICITY/ PRIVACY RIGHTS


Court Rules That Kids Can Be Bound By Facebook’s Member Agreement

By Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

The status of kids’ ability to form contracts via online terms of service was somewhat uncertain over the last several years, with a few Facebook-related rulings raising questions. A group of minor plaintiffs who opted out of the Fraley v. Facebook Sponsored Stories settlement brought suit for violation of their publicity rights under an Illinois statute.

A recent ruling shuts out their claims, and gives some clarity to the online contracting landscape for minors.

The key question in front of Judge Seeborg was whether the contract at issue between minors and Facebook — essentially granting a publicity rights release — was one of the narrow types of contracts with minors that were void, or if the contract was merely voidable under California Family Code 6701, et seq. Section 6701 sets forth certain exceptions to the general rule of contract voidability for minors—i.e., a minor cannot:

(a) give a delegation of power (b) make a contract relating to real property …
(c) make a contract relating to personal property not in the immediate possession or control of the minor

Plaintiffs tried to rely on subsections (a) and, as a fallback subsection (c), but the court quickly rejects these as inapplicable. As to whether entry into a TOS is a delegation of power, the court says it is no more so than any ordinary contractual arrangement. Sure, Facebook has the right to do certain things with the minor’s image and likeness, but this isn’t the type of delegation the statute is intended to cover. Subsection (c)’s reference to property that is not in the immediate possession of the minor means that it doesn’t apply to licenses.

Given that the contracts don’t fit into any of these (narrowly construed) categories that would render the contract void, the Facebook’s contract with the minors is voidable, meaning that it’s valid until the minors decide to void it. Plaintiffs made no allegations that they had tried to void it. In fact, the minors in this case:

[did not] dispute that they continued to use their Facebook accounts long after this action was filed.

With the caveat that this is just a district court ruling, and plaintiffs will continue to attack these terms in far-flung jurisdictions, this is a very helpful ruling for Facebook in that
it removes some uncertainty as to a big category of potentially lucrative users: users who are old enough to not pose COPPA-problems but those who haven’t yet reached the age of majority. Networks for the most part took a don’t-ask/don’t-tell type of approach with this group, but were hesitant to enter into deeper economic and legally uncertain relationships. (The litigation over in-app purchases serves to illustrate why these relationships can be challenging for networks. See In re Apple In-App Purchase Litigation. Facebook is also involved in a similar dispute, which is pending.)

One possible downside for networks and silver lining for minors: the right of dis-affirmance—that the plaintiffs failed to exercise here—could translate into a takedown right of sorts. It probably cannot be an effective tool to take down older content (see California’s minor “eraser law” for something that could come into play here), but it could certainly turn into a hassle for networks when it comes to continued ability to exploit content from a minor’s account. From a logistical standpoint, perhaps networks will simply decide that it’s easier to remove all content from a disaffirming minor’s account?

_____

**Eric’s Comments:** I think this is a significant ruling. The court says three important things:

1) the TOS is enforceable against minors until they void it. This is a big win for all online services, not only Facebook. 2) the only way minors can void the contract is by terminating their accounts. In some cases, litigious minor users will be happy to do that, but a site with strong lock-in effects like Facebook is relatively immune from widespread terminations. 3) The termination only applies to future activities, not past activities. So Facebook’s agreement protected Facebook’s Sponsored Stories usage prior to voiding.

This ruling isn’t limited to Facebook. It should apply to all online services (at least those governed by California law). This means that, as a starting point, minors will be bound by the risk allocation provisions in a website’s user agreement until the minors terminate the agreement, and that termination will not eliminate the risk allocation provisions for issues prior to termination.

This ruling isn’t entirely unprecedented. It’s consistent with the AV v iParadigms case from a few years ago. That case is noteworthy because it indicated that the kids couldn’t terminate the copyright license when they tried to void the contract (because the contract was “complete”). Thus, it’s possible that minors couldn’t force Facebook to remove the already-posted content by voiding the user agreement. Instead, they would be channeled to California’s terrible online eraser law, which may or may not permit their deletion depending on how service providers and the courts interpret its pathetically sloppy language.
Related posts:

Minors’ Suit Over Facebook Credits Continues – I.B. v. Facebook
Minors’ Suit Over Facebook Credits Survives in Part – I.B. v. Facebook
Facebook’s “Browsewrap” Enforced Against Kids–EKD v. Facebook.
Parents’ Lawsuit Against Apple for In-App Purchases by Minor Children Moves Forward — In re Apple In-App Purchase Litigation.
Clickthrough Agreement Binding Against Minors–A.V . v. iParadigms
Court Declines to Dismiss or Transfer Lawsuit Over @OMGFacts Twitter Account — Deck v. Spartz, Inc.

*   *   *

CONTENT REGULATION. DERIVATIVE LIABILITY

*   *   *

*   *   *


Employer Gets Section 230 Immunity For Employee’s Posts

By Eric Goldman

http://www.blog.ericgoldman.org

[Note: I am massively behind in blogging Section 230 cases. I probably have a dozen or so festering in my queue. C’est la vie. This case jumps to the front of the queue because of its recency and its relatively novel result.]

Miller is a member of the Indianapolis business community. The Indianapolis Business Journal published an online article covering the controversy over one of his projects. The article prompted three allegedly defamatory comments from anonymous users. Miller eventually learned that two of those comments were written by Dave Wilson, an employee of 500 Festival; and the other comment came from an unknown user of FedEx’s Internet access service. [The opinion doesn’t clarify if this is a commercial Internet access service or available only to employees.] Miller named 500 Festival and FedEx as defendants.

500 Festival and FedEx defended on Section 230 grounds. The flagship case in this area is the Delfino v. Agilent case from 2006, where the employer got Section 230 immunity for an employee’s online mischief unrelated to the employee’s job. The other case in this area is Lansing v. Southwest Airlines, which this court oddly treats as supporting precedent even though the Lansing court (in an ugly opinion) rejected the employer’s Section 230
defense against a negligent supervision claim. The court doesn’t discuss the Espinoza case, which distinguished Delfino in ways that reinforced that this case was factually similar to Delfino, or the Avery v. Idleaire case, which would have been adverse precedent as well.

The court says 500 Festival and FedEx both qualify for Section 230 immunity, following the typical Section 230 immunity three-part analysis:

1) Provider/user of ICS? Citing both Delfino and Lansing, the court says “both 500 Festival and FedEx provide or enable computer access for multiple users on their respective computer networks to access the Internet by means of the servers on each network. We conclude that this is all that is required under Section 230(c)(1) to be considered a provider of an interactive computer service.”

2) Another ICP (third party content)? “the information at issue—the comments posted to the IBJ website—was provided by another ‘information content provider’….FedEx’s unknown user and 500 Festival’s known employee, Wilson, easily fall within this definition.”

3) Publisher/speaker? “The Millers’ complaint clearly seeks to hold 500 Festival and FedEx liable for what they published….And despite their references to other doctrines, such as respondeat superior, the Millers’ actual complaint seeks to hold 500 Festival and FedEx liable as publishers of the statements.”

It’s nice to see that the terrible Lansing opinion is being used for good rather than evil. I used to think the Delfino opinion was abberational, but this opinion builds on it to reiterate that employers could qualify for Section 230 immunity for their employees’ online activities. That’s a result that should grab attention from employment lawyers (both plaintiff- and defense-side).

* * *

CONTENT REGULATION, INTERNET HISTORY, SEARCH ENGINES


Of Course The First Amendment Protects Baidu’s Search Engine, Even When It Censors Pro-Democracy Results

By Eric Goldman

http://www.blog.ericgoldman.org

Baidu.com is the leading search engine in China. The plaintiffs in this case have published materials online about the democracy movement in China. They allege that, at the request of the Chinese government, Baidu excludes pro-democracy search results, including their materials. They sued Baidu in the United States for this alleged censorship. Recently,
in a scholarly, thoughtful and wholly persuasive opinion, a federal judge emphatically rejected the lawsuit, saying the First Amendment protected Baidu’s search results.

To me, the First Amendment’s application to search results isn’t even a close question. Search engines “publish” their search results. Like all other media publishers, search engines decide what content to include and exclude and how to prioritize that material. As the court says,

there is a strong argument to be made that the First Amendment fully immunizes search-engine results from most, if not all, kinds of civil liability and government regulation. The central purpose of a search engine is to retrieve relevant information from the vast universe of data on the Internet and to organize it in a way that would be most helpful to the searcher. In doing so, search engines inevitably make editorial judgments about what information (or kinds of information) to include in the results and how and where to display that information (for example, on the first page of the search results or later).

Indeed, the plaintiffs acknowledged that Baidu exercised editorial judgment when it allegedly deliberately excluded their content. It’s just that they wanted Baidu to make a different editorial choice. Furthermore, the plaintiffs acknowledged that users could find their content on other search engines, which reminds us that search engine users should experiment with different search engines to determine which ones are most helpful.

The court says the fact that search engines instantiate their editorial judgments into algorithms is legally inconsequential. As the court notes, “the algorithms themselves were written by human beings.” Yet, for reasons that perplex me, some folks feel the rules should change for algorithm-mediated speech. Perhaps we irrationally fear algorithms because we expect them to go rogue on humans (e.g., HAL in the movie 2001), or because the surreptitious black-box nature of search engine algorithms arouses suspicions (even though human editors are just as “black box” about how they make their editorial judgments). I’d like to think we’re moving past those techno-panics, but Google’s increasing market share seems to be exacerbating the paranoia.

This ruling’s application of the First Amendment to search results isn’t unprecedented. In fact, the Search King v. Google case reached that conclusion over a decade ago; as did another case in 2007. This opinion doesn’t address 47 USC 230(c)(2), a law Congress passed in 1996 to eliminate websites’ liability for their filtering decision (see my essay on that law). That law also protects search engines’ filtering decisions, as the 2007 opinion ruled. Given the overlapping Constitutional and statutory protections for search engine publication choices, this lawsuit never seemed tenable.

In addition to its lack of legal merit, I find activist lawsuits like this troubling for two reasons. First, the lawsuit is really a political protest over Chinese censorship, but the battle
is being waged by proxy against a private entity allegedly complying with its government’s laws. Regardless of how you feel about government censorship, a private lawsuit against a commercial actor isn’t the right way to fix it. Better mechanisms would be to keep encouraging the Chinese government to rethink its policies, and to encourage the development of pro-freedom technologies that give Chinese Internet users more choices.

Second, the lawsuit’s underlying objective is to export our free speech norms to China. I favor free speech so strongly that this sounds good to me, but recognize the potential duplicity when another country tries to impose its cultural norms on us. For example, in LICRA v. Yahoo, French activists sued Yahoo for enabling the resale of items celebrating the Nazi party on Yahoo.com operated out of servers in California. The case eventually sputtered in court, but many Americans resented that France would tell us in the United States what was culturally appropriate for our country. The Baidu lawsuit is the mirror image of LICRA v. Yahoo, except we’re exporting US norms to China rather than France exporting its norms to the US. If you don’t like France telling us what our cultural norms should be, you’ll want to figure out in your head how the Baidu lawsuit differs. [Note: I’m putting aside the unavoidable hypocrisy about the United States’ stance on censorship given the many efforts our government has pursued to increase Internet censorship.]

For further perspectives on the legal regulation of search engine results, see my 2006 article on search engine bias (cited by the court) and my 2011 revisit of the topic.

* * *

EVIDENCE/ DISCOVERY, LICENSING/ CONTRACTS


How To Get Your Clickthrough Agreement Enforced In Court

By Eric Goldman

http://www.blog.ericgoldman.org

So, by now, you know that if you want an enforceable online agreement, you need to implement it as a mandatory clickthrough. With that settled, it’s time to address an advanced topic: what evidence can you offer a judge to uphold your clickthrough when plaintiffs challenge the mechanical aspects of its implementation?

I recently addressed the evidentiary question in my post about JDate’s member agreement. The plaintiff alleged that she remembered agreeing to a different venue selection clause than the one invoked by JDate. In response, JDate introduced:
a sworn statement from its North American Director of Customer Support that the “Terms of Service were applicable to all subscribers of Spark Networks’ website at JDate.com and no material changes were made thereto during all four periods where Ms. Zaltz was a subscriber of Spark’s website at JDate.com” and the forum selection clause at issue was part of those Terms of Service and “remained unchanged during Ms. Zaltz’s subscription to JDate.com.”

This evidence was sufficient to get JDate’s venue selection clause enforced in a motion to transfer.

Recently, Hotwire’s clickthrough agreement survived a similar legal challenge. The court’s discussion (citations omitted and emphasis added):

It is undisputed that Plaintiff used the Hotwire website on December 15, 2012 to book his car rental for Mexico. Plaintiff argues that Defendants have not met their burden to demonstrate that he agreed to the forum-selection clause contained in the Terms of Use. Specifically, Plaintiff alleges that Hotwire may have made a false representation in his access to the Terms of Use and argues that perhaps the hyperlink was not functioning properly at the time Plaintiff made his purchase. Defendants have produced two declarations from employees at Hotwire: (1) Sarah Bernard who at the operative time was the Vice President of Product Management for Hotwire; and (2) Jacob Aaron Joachin Hadary who was the Lead Product Manager for Hotwire during that time. Bernard and Hadary affirmatively state that the Terms of Use in operation during the December 2012 time frame included a forum-selection clause. Hadary declares, and corroborates Bernard’s declaration, that an individual using the Hotwire website cannot complete a booking without checking the “Acceptance Box” acknowledging the acceptance of “Hotwire’s terms and conditions and other applicable rules.” Hadary confirms that this requirement has been in place since 2005. Plaintiff confirms that he completed his booking through the Hotwire website which indicates that he checked the Acceptance Box. The language in the Acceptance Box shows that even though the terms were provided by hyperlink Plaintiff acknowledged accepting the “terms of use and Hotwire’s” rules. The Court concludes that, in the absence of an affirmative denial from Plaintiff that he did not in fact check the Acceptance Box and clear evidence that Plaintiff could have not otherwise completed his car reservation, Plaintiff had notice and consented to the Terms of Use containing the forum-selection clause. The Court finds that the parties agreed to the forum-selection clause contained in the December 2012 version Terms of Use and it is therefore valid.

I don’t understand why the court suggests that the plaintiff’s denial of checking-the-box would be relevant. Every plaintiff trying to defeat an online user agreement will make
that denial, true or not. I believe a plaintiff should have to offer more rigorous/less self-serving evidence if it wants to legitimately rebut Hotwire’s evidence enough to create a meaningful factual dispute.

Either way, this ruling reinforces that simply having an airtight clickthrough agreement isn’t enough. You also should have a reliable chain of evidence to show (1) the agreement’s terms on any specific date, and (2) what user interactions were technologically required to manifest assent on that date. You should also assume that you’ll need to be able to introduce this evidence even if all of the relevant employees have gone elsewhere by the time the matter gets into court.

**Related posts:**

* Court Rules That Kids Can Be Bound By Facebook’s Member Agreement
* Court Blesses Instagram’s Right to Unilaterally Amend Its User Agreement—Rodriguez v. Instagram
* Effort to Game Website User Agreement Rules Fails — Traton News v. Traton Corp.
* JDate Member Agreement Upheld—Zaltz v. JDate (Forbes Cross-Post)
* How Zappos’ User Agreement Failed In Court and Left Zappos Legally Naked (Forbes Cross-Post)
* Court Disregards Check-the-Box Agreement and Doesn’t Enforce Venue Clause — Dunstan v. comScore
* Forum Selection Clause in “Submerged” Terms of Service Presumptively Unenforceable — Hoffman v. Supplements Togo
* Second Circuit Says Arbitration Clause in Terms Emailed After-the-Fact Not Enforceable – Schnabel v. Trilegiant
* Clickthrough Agreement With Acknowledgement Checkbox Enforced—Scherillo v. Dun & Bradstreet
* Contract Formed Even If Customer Never Received It–Schwartz v. Comcast

* * *
E-COMMERCE, LICENSING/CONTRACTS. MARKETING, PRIVACY/SECURITY

In re LinkedIn User Privacy Litigation, 12-CV-03088-EJD (N.D. Cal. Mar. 28, 2014)

Privacy Claims Based on LinkedIn’s Security Promises Survive Motion to Dismiss

By Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

This is a lawsuit filed in the wake of a widely reported data breach at LinkedIn. Plaintiffs alleged benefit-of-the-bargain type claims against LinkedIn, saying LinkedIn failed to live up to its security practices. The first time around, the court rejected these claims and granted LinkedIn’s motion to dismiss. (“Court Dismisses Data Breach Lawsuit Against LinkedIn Based on Compromised Passwords – In re LinkedIn User Privacy Litigation.”) This time around, the named plaintiff slightly adjusts her pleadings, and part of her claim survives.

Standing: She alleges that she was a premium subscriber from March through August 2010 and that:

prior to her purchase of the premium subscription, she read LinkedIn’s User Agreement and Privacy Policy and that, had LinkedIn disclosed its lax security practices, she would have viewed the premium subscription as less valuable and would have attempted to purchase a premium subscription at a lower price or not at all.

The court says that the cases construing California’s unfair competition statute hold that a consumer’s reliance on a product label is sufficient to confer standing under both the UCL and Article III. LinkedIn, on the other hand, argued that this precedent only applies to cases where the misrepresentation is contained in a “label or an advertisement.” While LinkedIn cited to cases saying that plaintiff has to allege more than “mere overpayment,” LinkedIn also disputed the notion that the statements in LinkedIn’s privacy policy was the type of advertising that could support a claim under the UCL statute at all. Among other things, the purported promise is a stray sentence that applies to premium and non-premium members alike. The court rejects LinkedIn’s argument, taking a broader view of the Unfair Competition Law cases. The court says that cases aren’t strictly limited to misrepresentations in labels or advertisements; and even to the extent they are, the term “advertisement” is broadly construed. The court hints at some skepticism as to who would actually read the policy, but says that this is not the situation where a prospective customer was physically precluded from reading the policy.

Plaintiff states a claim: LinkedIn raised a variety of arguments on the merits, including that the representation in question was not material, that the precise method of data encryption was disclosed, and that this isn’t something that would register with an average
consumer. None of these is sufficient at the motion to dismiss stage. Plaintiff alleged “plaus-
sible” explanations and arguments for why the statement was false and would be likely
to mislead customers, and that’s the extent of the court’s inquiry. As to her explanation
of falsity, the court cites to the fact that (1) LinkedIn’s encryption practices were not in
line with prevailing industry recommendations (by the National Institute of Standards and
Technology), and (2) a few days after the data breach, LinkedIn publicly stated that it would
revise its encryption practices to bring them in line with prevailing industry standards.

The court dismissed the breach of contract and UCL claim based on the unfairness
prong previously, and dismisses those claims with prejudice. The UCL claim based on the
fraud prong survives.

The idea that flowery language in a privacy policy would come back to haunt a com-
pany is not entirely shocking. Nevertheless, that privacy policy language could potentially
support a claims under the UCL statute will probably raise a few eyebrows. As is frequently
said, there is no greater lie on the Internet than “I read and agreed to the terms and condi-
tions”! Interestingly, LinkedIn did not cite to or try to marshal any disclaimers or other
protective provisions in its terms of service to neutralize or otherwise undermine plaintiff’s
claims.

Privacy plaintiffs who happen to be paying customers are continuously fine-tuning their
claims, and it was inevitable that they would find some sort of hook, at least to survive a
motion to dismiss. To their benefit, the theory advanced doesn’t require a showing of harm
flowing from the breach – i.e., they need not show that their information was ultimately
misused. But they would have to prove up their allegations that they read and relied on the
policies in question, and that’s where they will face some serious challenges. The case may
also not lend itself to class resolution, and this may derail the case as a class action as well.
(See the Gmail privacy litigation ruling.)

Eric’s Comments: First, my apologies to Venkat and all of you for my delay adding these
comments. Venkat wrote this post 5 weeks ago and I’ve held it up. Sorry.

The ruling involves the following sentence from LinkedIn’s privacy policy:

[all information that you provide will be protected with industry standard protocols and technology.

I’m sure most privacy policy drafters are wondering where the rest of the problematic
language is. As quoted, this is just harmless puffery, right? There’s no single definition of
“industry standard” or, for that matter, “protected.” It probably seemed inconceivable to
the drafter that this piece-‘o’-fluff could have any legal consequences.
But let’s look more closely at the plaintiff’s claims. The plaintiff says, apparently in earnest, that LinkedIn failed to salt passwords before hashing them—and if LinkedIn had disclosed its failure-to-salt, it would have affected the plaintiff’s decision to obtain LinkedIn’s premium services.

HAHAHAHAHA! After I stopped laughing uncontrollably, I have to call BS on that. I see one of two explanations here: (1) the plaintiff is the one-in-a-zillion potential customer of LinkedIn premium services that (a) would read the LinkedIn privacy policy all the way down to the puffy statements about security, (b) would know LinkedIn’s security practices were below industry-standard if LinkedIn disclosed that it encrypts passwords without salting them, and (c) would change the subscription decision because of the salting omission; or (2) the plaintiff is just feeding the judge a line to get past a motion to dismiss.

Neither assessment is likely to support a plaintiff victory. If it’s the latter, Rule 11 seems too gentle. If it’s the former, the plaintiffs’ lawyers won this round but apparently have made class certification almost impossible. At minimum, the class apparently now has serious typicality problems because the class representative is a unicorn.

To overcome the unicorn problem, the plaintiff argued that if LinkedIn had made proper disclosures, someone else would have publicized LinkedIn’s sub-industry standard practice well enough to change the plaintiff’s decision. This is an example of the tautologies that all-too-frequently plague false advertising litigation (“if I had known, I would have paid less” is another example). This argument works with respect to every alleged misrepresentation, i.e., I wasn’t able to understand things, but some unspecified beneficent third party would have understood the key truthful fact I needed to know and would have relayed this issue to me in a way that I could understand. Even if this impossible-to-refute tautology works to defeat the motion to dismiss, it should hinder class formation for all of the reasons discussed in Judge Koh’s Gmail ad privacy ruling.

So this opinion made me want to laugh and cry simultaneously. I wanted to cry because this lawsuit survived when it shouldn’t have; and it survived on assertions that seem mockably dubious. At the same time, I wanted to laugh at the plaintiffs for virtually ensuring the case will lose in a future round—meaning the plaintiffs are investing more bucks in a zombie case (i.e., a case that’s already dead based on their factual concessions).

What’s not funny at all is the legal system’s treatment of puffy statements about an Internet company’s security practices. We’ve already seen how the FTC and state AGs are masters at making jaw-droppingly tendentious interpretations of these statements. Now we can see how class action lawyers will do ANYTHING to chase down the puffery, even if it means finding LinkedIn subscribers who would drop services for failure-to-salt. We’ve
said it before, but it bears reminding: the security provisions in your privacy policy should contain only verified facts and ZERO innuendo. If you haven’t scrubbed your privacy policy recently to de-puff it, time’s a-ticking.

[Disclosure: I am now a LinkedIn Influencer, which includes the perk of getting a free premium subscription.]

**Venkat’s surreply:** The idea of relying on representations in a privacy policy is laughable to me as an average consumer. However, I do wonder when it comes to privacy and security practices whether *something* needs to deter companies into being less cavalier. (See, e.g., Snapchat.) Class actions are a terrible tool in this context (see “The Irony of Privacy Class Action Litigation”), but given that other tools have been ineffective, maybe it’s not such a bad thing to create some fear in the minds of company privacy officers?

As for Eric’s newly-minted status as a LinkedIn Influencer, a hearty congratulations to him. If he would promise to bring the classic Eric Goldman snark (which I suspect is very unlikely), I would gladly follow his writings there.

* * *

**DERIVATIVE LIABILITY, E-COMMERCE, MARKETING, PRIVACY/SECURITY**

*Opperman v. Path*, 2014 WL 1973378 (N.D. Cal. May 14, 2014)

**Apple May Be Liable For Privacy Violations by Third Party Developed Apps**

By Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

There are so many privacy lawsuits around the iOS ecosystem that it’s tough to keep track of them all. This particular (consolidated) lawsuit involves privacy claims against Apple and also against various apps, including Angry Birds, Cut the Rope, Facebook, Path, Foodspotting, Foursquare, GoWalla, Twitter and others. Apple and the app developers both moved to dismiss, and the court grants the motions, with the exception of an invasion of privacy claim against the app developers.

While the plaintiffs are given a chance to amend, they should consider packing this one up and heading home.

**Apple:** Apple first argued that plaintiffs failed to satisfy standing because they did not identify specific representations from Apple that caused plaintiffs to overpay for the iOS devices. The court says that Apple conflates standing with the merits of the claims.
Additionally, plaintiffs can establish standing through statutory violations (citing Edwards v. First American). Finally, Apple cited to a ruling in a privacy lawsuit against LinkedIn for the proposition that plaintiffs alleging overpayment claims have to allege “something more”. The court says this reads the LinkedIn case too broadly, and in any event, plaintiffs had alleged something more (that the iOS platform was designed to allow easy access to personal information).

Apple also raises a Section 230 defense, which we wondered about when we first flagged the case. The court cites to the usual Section 230 standards, but ends up concluding that the amended complaint:

pleads sufficient conduct to classify Apple as an ‘information content provider’ whose conduct is not protected by the CDA.

As support for this proposition, the court cites to Apple’s iOS guidelines that “appear to encourage the practices Plaintiffs complain of in this case.” The court cites to portions of the guidelines and tutorials where Apple teaches and encourages plaintiffs to “code and build apps that non-consensually access, manipulate, alter, use and upload the mobile address books maintained on Apple iDevices.”

Finally, Apple argues that plaintiffs failed to adequately allege misrepresentations, or identify specific statements that plaintiffs relied on. Although in a previous order the court denied Apple’s motion to dismiss on this point, the court revisits the issue and this time around says that the representations are indeed lacking. Plaintiffs vaguely alleged that they “viewed the Apple website,” but this is short of identifying a specific representation that influenced their purchasing decision. Plaintiffs alternatively argued that their allegation of a “long-term” advertising campaign containing deceptions that relieve them of their obligation to satisfy the specificity requirement, but the court rejects this argument.

The court also tosses the remaining claims against Apple: (1) claims under California’s anti-hacking statute, section 502 (for failure to allege that Apple circumvented a technical or code-based barrier); (2) design defect/failure to warn (failure to allege harm to person or property); (3) negligence (economic loss rule); and (4) aiding and abetting (no facts other than those previously alleged that support any theory of aiding and abetting).

**App Defendants**: The App defendants also raised standing arguments, but the analysis differed slightly between the court’s discussion as to Apple and the discussion as to the app defendants. As to these defendants, because the apps were free, plaintiffs could not allege that they were out any money. As a result, they faced more of a challenge in satisfying
standing. The court rejects their theories that standing could come from (1) their request for injunctive relief or (2) interference with their “property rights in their address books.”

Nevertheless, the court finds that they satisfy standing on two different grounds. First, they allege statutory violations, and this is sufficient under Edwards v. First American to satisfy standing. Second, they allege invasion of privacy, which the court says is sufficient to confer standing as to that claim. As to the invasion of privacy claim, the court says that plaintiffs did have a reasonable expectation of privacy in their contact information and address books. The app defendants argued that their access of the contact information was not “highly offensive” to the reasonable person, but the court says it is unable to conclude that as a matter of law. The app defendants also argued that plaintiffs failed to adequately allege damages, but the court also says that this is not amenable to resolution at the motion to dismiss stage. The court does say that plaintiffs’ theory of public disclosure of private facts is not sufficient because there was no allegation that the contact information was disclosed to the public at large. *The intrusion of seclusion invasion of privacy claim survives.*

Finally, the court gets rid of the various statutory claims. The CFAA and Section 502 claims fail because plaintiffs failed to allege lack of authorization. The ECPA claim, as well as the Texas and California wiretap claims, fail because there was no “interception.” Plaintiffs also alleged a claim under a Texas theft statute, but the court says that plaintiffs can’t satisfy the “deprivation” element of a theft claim.

**Facebook and Gowalla Motions:** The Facebook and GoWalla motions focused on whether Facebook would be held liable as a result of acquiring GoWalla and whether GoWalla’s sale to Facebook somehow constituted a fraudulent transfer. As to the first claim, the court says after reviewing a copy of the Facebook-Gowalla agreement (under seal), that Facebook transferred cash and pre-IPO stock to GoWalla, in exchange for a non-exclusive royalty-free license to GoWalla’s patents. The agreement did not convey to Facebook any title to GoWalla intellectual property. Thus, there was no “transfer” within the meaning of the uniform fraudulent transfer act. Plaintiffs also failed to allege that the transfer put any assets that plaintiffs would be able to execute their prospective judgment against beyond their reach. The argument for successor liability fails as well because plaintiffs failed to allege that Facebook acquired GoWalla and failed to allege a transfer of assets.

---

The address book lawsuits always struck me as the classic privacy lawsuit that was unsupported by any real harm. The idea that Apple should be held liable for these supposed
harm is a crazy stretch, but as always, plaintiffs latched on to flowery marketing language in an attempt to construct a claim.

Fortunately, the court isn’t having it, but unfortunately, the court throws in some Section 230 discussion that probably has Professor Goldman cringing. The analysis should be two-fold: (1) Section 230 bars most attempts to hold Apple liable for information it makes available—i.e., the apps; (2) to the extent it makes contractual promises, it can be held liable for those promises. Instead, the court looks to Apple’s guidelines to developers and casts this “conduct that goes beyond the traditional editorial functions of a publisher.” I’m not sure exactly what the court means here, and whether the court is trying to stretch the 9th Circuit’s Roommates opinion, but it’s somewhat out of left field, and contrary to the well-established body of Section 230 jurisprudence.

The app developers are dealing with claims from free customers, so they are able to rely on standing, but only to a certain extent. Even still, with the exception of the privacy ruling, the court’s treatment of the remainder of the claims is fairly unsurprising. As to the invasion of privacy ruling, I suppose the court could have gone either way at this stage, given the malleability of a standard such as “shocking to the reasonable person.” But I would think most people would find surprising the conclusion that access by the apps of your address books could be “highly offensive”. (Cf. “Court: Husband’s Access of Wife’s Email to Obtain Information for Divorce Proceeding is not Outrageous“.) Perhaps the result should be different if the apps take those address books and misuse the information in them, but for the most part, there is no credible evidence that the apps ever exploited this information, either internally or externally, beyond facilitating interactions with contacts. As a result, although these claims get past the motion to dismiss stage, I can’t imagine they will withstand a motion for summary judgment. Not to mention that they may suffer from the defect that they are probably not amenable to class-wide resolution. In any event, this lawsuit still continues to limp along.

**Related posts:** Google Wins Cookie Privacy Lawsuit

Judge Boots Privacy Lawsuit Against Pandora but Plaintiffs Can Replead – Yunker v. Pandora

$1 Billion Pro Se Privacy Lawsuit Against Google Fails–Shah v. MyLife

Judge Koh Whittles Down iPhone App Privacy Lawsuit – In re iPhone Application Litig.

Reidentification Theory Doesn’t Save Privacy Lawsuit–Steinberg v. CVS Caremark

App Developer RockYou Settles Privacy Lawsuit–Claridge v. RockYou
Comments on Doe v. IMDB Privacy Lawsuit

Google Gets Dismissal of Lawsuit Over Privacy Policy Integration—In re Google Privacy Policy

Court Dismisses Data Breach Lawsuit Against LinkedIn Based on Compromised Passwords— In re LinkedIn User Privacy Litigation

Men’s Journal Beats Lawsuit Alleging Violation of California’s “Shine the Light” Privacy Statute — Boorstein v. Men’s Journal

New Essay: The Irony of Privacy Class Action Lawsuits

TheDirty Defeats Privacy Invasion Lawsuit–Dyer v. Dirty World

Privacy Claims Based on LinkedIn’s Security Promises Survive Motion to Dismiss

Another Questionable IP Lawsuit Over a Derogatory Twitter Account

Android and Pandora Privacy Rulings Accept Low Hurdle for Standing

Employer Who Takes Over Employee’s Social Media Accounts May Commit Privacy Violation–Maremont v Susan Fredman Design

Sony PlayStation Data Breach Lawsuit Whittled Down but Moves Forward

Is Sacramento The World’s Capital of Internet Privacy Regulation? (Forbes Cross-Post)

Video Privacy Protection Act Plaintiffs Can Proceed Against Hulu Absent Showing of Actual Injury

*   *   *

Measuring The Bull’s-Eye On Target’s Back: Lessons From The T.J. Maxx Data Breach Class Actions

Randy Maniloff

White and Williams, LLP

www.CoverageOpinions.info

Once my wife believes something it is very difficult to change her mind. And if her mother agrees with her then look out. I could call in Socrates to speak with her and even he would walk away just shrugging his shoulders. Sorry man, I tried.

In a way this is the situation that Target Corp. is going to face when it defends the 70 or so putative class actions that have recently been filed against it—so far—in various federal
courts around the country for damages allegedly caused by a massive security breach of its customers’ personal and financial information. Yes, 70. You read that right.

At issue is the theft of the retailer’s customers’ personal information from the magnetic strips of their credit and debit cards. The theft allegedly occurred between November 27 and December 15 when customers’ cards were swiped through the retailer’s point-of-sale terminals. This was no small data breach. In general, it was initially announced that thieves stole credit and debit card information from 40 million customers. It later came to light that the same criminals acquired names, addresses and phone numbers from as many as 70 million accounts. However, given the no doubt overlap of these two groups, the number of affected individuals is not 110 million. Not that that’s much of a consolation for Target. And just as day follows night, after the breach was announced, the law suits began rolling in. Seven were filed on the same day that the breach was announced. For some plaintiffs’ lawyers this was the Black Friday door bust to end all others.

Despite the parade of horribles that the class action complaints allege that Target caused to its customers, Target’s website states that its guests (as the company refers to its customers) will have “zero liability for any charges that [they] didn’t make.” Target’s CEO, Gregg Steinhafel, in a CNBC interview that aired Monday, repeated that over and over and over. There’s no ambiguity there. No Target customer will be picking up any bar tabs in Nigeria.

But none of this will matter to the plaintiffs’ attorneys that have filed the class action suits. Just as my wife will never be convinced that taking Montgomery Avenue home from the King of Prussia Mall is just as good as Old Gulph Road, the plaintiffs’ attorneys will never believe that Target, no matter what it says or does to try to convince them, will adequately compensate its customers. [Actually, they probably do. But if they said so it would leave no compensation for themselves. So the class action suits will roll on.]

At least Target’s shareholders feel confident that the retailer will make all of this right. The company’s stock has held up well despite the onslaught of negative publicity and obvious fact that the data breach is going to cost Target shopping carts full of money. [Target’s revenue in 2013 was $73 billion. That’s more than the gross national product of over a hundred countries. So the company is unlikely to feel the hit as much as some would.]

Target is going to experience financial exposure on many fronts. Some of the obvious ones are the cost to investigate the data breach and upgrade its systems to prevent future breaches. There will be lost sales, which will translate to lost profits. Target has reported that it expects fourth quarter 2013 adjusted earnings per share of $1.20 to $1.30 compared with prior guidance of $1.50 to $1.60. Target will face claims from banks that suffered losses for fraudulent charges, as well as for the cost of banks to issue replacement cards. [A
recent Wall Story Journal story addressed some issues surrounding that last point.] Target may be required to deal with shareholder suits against the company as well as settlements with state attorney’s general.

And, of course, Target will surely be required to compensate its customers for their alleged damages. These 70 or so class actions and counting are not going to be litigated in any court of law with a jury foreperson someday standing up and announcing a verdict in favor of Target. Of course not. These class actions will be settled. Target is much too reputation-dependant to not want to get these suits in the rear view mirror pronto.

So how might the Target class actions play out? That is impossible to gauge at this point. But for some guidance on that question consider the 25 class action complaints, filed in 2007, against retailer T.J. Maxx (and some sister stores), for damages allegedly caused by the theft of customers’ personal information.

But before getting to the TJX cases, and what they may foretell for Target, it is worthwhile to look at the Target class action complaints themselves and address whether Target has done what’s alleged and whether the plaintiffs have in fact suffered the damages they claim. Not that any of these details matter in the world of consumer class actions, but just indulge me.

The class action plaintiffs seek damages for their financial losses due to unauthorized charges on their credit and debit cards. But Target has made it abundantly clear that its customers will suffer no such losses. The class action plaintiffs also seek to be provided with credit monitoring services. That is usually one of the more tangible elements of damages sought in cases like this. Target has stated that it will offer free credit monitoring to its customers for one year. Details of this are spelled out on Target’s website. The company didn’t need to be forced by any court to offer this service.

Some class action plaintiffs seek damages for emotional distress. Really. I’m not making that up. My wife shopped at Target during the breach period. Thankfully she seems to be holding up just fine. But I am keeping a close eye on her for any changes in her behavior.

Some plaintiffs are seeking punitive damages from Target. But it is inconceivable that anything Target did could justify punitive damages. You don’t get to be the nation’s second largest retailer, with over 1,900 stores, by acting in any manner that comes within a hundred miles of conduct that could justify punitive damages.

The class action plaintiffs allege that Target breached various state consumer protection statutes. But these statutes are likely inapplicable to the circumstances here and/or Target did not act with the level of culpability required to have committed such a breach. The class action plaintiffs also allege that Target breached various state statutes that require
timely notice of a data breach. Target announced the breach just four days after it was discovered. Further, these statutes generally do not include a private right of action.

Most reasonable people would stop shopping in any store that treated them as horribly as they alleged Target did. But I suspect that the class action plaintiffs have not seen the last of the inside of a Target store.

But despite the assurances and benefits that Target has offered voluntarily, without any court intervention, the class actions are still sure to settle—and for some big numbers. Judge William Young, a Massachusetts federal judge, has stated: “Simply put, the class action vehicle is broken.” That Judge Young made this statement, in the context of overseeing the T.J. Maxx data breach class actions, does not bode well for Target. See In Re TJX Companies Retail Security Breach Litigation, No. 07-10162 (D. Mass. Nov 3, 2008).

While the Target consumer class actions are bound to settle, what might that look like? Again, while it is impossible to know at this point, the settlement of the T.J. Maxx data breach class actions sheds some light on what may lie ahead for Target.

The T.J. Maxx data breach involved the theft of data related to over 45,000,000 credit and debit cards used at TJX Stores (T.J. Maxx, Marshalls, HomeGoods and a few others). However, banking associations that issued some of the affected cards asserted that hackers actually compromised the security of over 94,000,000 accounts. In any event, TJX announced in January 2007 that some customer financial information, as well as driver’s license numbers (which may be the same as social security numbers) were stolen from its systems.

Twenty-five class actions were filed and settled swiftly. Target is also likely to address the class actions with similar alacrity as TJX. In general, the settlement terms were as follows.

TJX offered three years of Equifax’s “Credit Watch Gold with 3-in-1 Credit Monitoring” (which includes $20,000 in identity theft insurance) to the approximately 455,000 class members whose name, address and driver’s license or military, tax or state identification number (which for some is the same as their social security number) may have been compromised. These are individuals who had previously returned merchandise to TJX without a receipt and, as part of that process, had provided such information to the retailer (the so-called “unreceipted return customers”). Such credit monitoring had a retail price of $390 for each class member. Thus, the cost to provide this service to 455,000 class members was $177,000,000.
But here’s the rub. According to the court’s opinion addressing attorney’s fees (approved to be $6.5 million; but subject to a very lengthy explanation from the court), only slightly more than 3% claimed the credit monitoring benefit.

Target is now offering its customers one year of Experian’s ProtectMyID credit monitoring, which includes $1,000,000 of identity theft insurance. According to Experian’s website, the retail price of this is $15.95 per month. Of course, Target is obviously not paying the rack rate.

It is not surprising that only slightly more than 3% of the eligible TJX class members sought credit monitoring. It was offered to them eons after the data breach took place. By the time it was offered those affected either forgot about the breach or knew by then that they were probably not in an jeopardy of identity theft.

Target’s offer of credit monitoring is world’s apart from TJX’s. Target is offering it to all of its customers and doing so when the incident is very fresh in their minds. Indeed, Target’s offer is coming while the data breach story is still front page news. There are exponentially more than 455,000 people eligible for credit monitoring and a lot more than 3% are going to take Target up on its offer. Consider that you aren’t even required to have shopped at Target during the breach period to sign up for credit monitoring. I didn’t shop at Target during the relevant period and I just signed up for it. The process was really easy.

Target is voluntarily taking on a huge credit monitoring expense. Target could do what TJX did and offer credit monitoring as part of a class action settlement long after this incident has been forgotten. This would dramatically reduce its credit monitoring liability. But that’s not the path it took. Nonetheless, despite voluntarily approaching credit monitoring in this manner, that likely won’t be enough for the class action plaintiffs’ attorneys.

The TJX settlement also included various cash payments and store vouchers for these unreceipted return customers. TJX reimbursed any costs incurred to replace their driver’s license. Those whose social security number was the same as their driver’s license, military, tax or state identification number could recover losses over $60 that occurred as a result of identity theft traceable to the breach. Customers were required to submit proof of loss and the aggregate amount payable for this category of damages was $1,000,000. As of the court’s November 3, 2008 opinion addressing attorney’s fees, almost 4,800 of such claims had been made. None were deemed valid and no payments had been made under this category.

Another category of benefits was offered to customers who certified that they made a purchase with a credit card, debit card, or check at TJX stores during the relevant time periods and incurred at least $5 in out-of-pocket expenses or lost time (valued at $10 an hour)
as a result of the intrusion. Under this “self-certification” option, class members needed only to state, under penalty of perjury, that they had made a check or card purchase and that they had suffered the required loss. These individuals would receive, at their option, either a $15 check or a $30 voucher. The agreement imposed a $10,000,000 cap on claims made by self-certifying class members. Claims were valued at $30, whether for check or voucher. Class members who could provide documents that they both made a qualifying purchase (for example, a credit card statement) and suffered the requisite loss were eligible to receive a $30 check or $60 in vouchers. The agreement imposed no cap on the value of vouchers that class members could claim via this method but limited the payout made in check form to $7,000,000.

For lawyers who no doubt claimed that a data breach was a huge inconvenience for customers, they sure didn’t put a lot of value on their clients’ time or inconvenience when it came to reaching a settlement. Ironically, for most TJX customers, making a claim for compensation was probably a bigger inconvenience than the data breach itself ever caused them.

It is hard to imagine Target not voluntarily offering its customers some sort of coupons as an apology, for their inconvenience, as evidence of taking responsibility and a sign of good faith to win back their loyalty. Target already offered its customers a 10% discount the weekend after the breach was announced.

So what does all of this mean for Target. The simple answer is this. Even if no Target customer will have any liability for fraudulent charges; even if Target takes on a huge credit monitoring liability—and far greater than if it waited to be compelled to do so; even if the consumer protection and data breach notice claims have no merit; even if the TJX case shows that actual losses for identity theft from a date breach are rare; and even if Target voluntarily offers compensation for inconvenience, none of this is likely to be enough to escape also paying the class action piper. That’s just how it works. The plaintiffs’ attorneys are not going to look at Target’s voluntary compensation and drop their cases. OK, this looks good. We’re not needed here. Move along folks. Nothing to see. What Target can hope for is that all of its voluntary compensation serves to take some of the value out of the class action settlements.

* * *
Just How Many Cyber Policies Are Floating Around Out There? (Not Nearly As Many As You Are Being Told)

Randy Maniloff

White and Williams, LLP

www.CoverageOpinions.info

Sometimes there are questions for which nobody knows the answer. And sometimes there are questions to which I know the answer but wish I didn’t—like how many Girl Scout Thin Mint cookies I ate last night.

One question in the Tootsie Roll Tootsie Pop category is how wide-spread are cyber or data breach insurance policies? There is one answer to this question that has been put forth: 31% of U.S. companies have such policies. This number comes from a 2013 report prepared for Experian—the people in the credit score and identity theft protection business. This number has been cited in articles appearing in The Financial Times (February 21, 2014) and The Wall Street Journal (December 3, 2013) and countless other stories on the web.

Looking at another source, an unnamed insurer participant, at a U.S. Department of Homeland Security cyber insurance workshop in October 2012, stated that only about 25% of companies have a cyber policy. [The report from this Homeland Security cyber insurance conference is interesting. If you poke around on the internet you’ll find it. But warning—you must remove your shoes to be allowed to read it.] A Law360 article on February 21st cited to a cyber lawyer’s conclusion that 25% of the property—casualty market has purchased cyber coverage. According to the Insurance Information Institute, the net written premium in 2012 for the property-casualty section of the insurance industry (auto, home and commercial) totaled $456 billion.

If Experian’s 31% conclusion is the right number, then of the pizza place, bagel store and burrito shop in the strip center near my house, one of these three businesses has an insurance policy to protect against the various risks of a data breach or cyber attack. The moon is more likely made of cheese. I decided to take a closer look at the Experian report—in other words, the report itself and not the media portrayals of it. My conclusion: The Experian report has led to false impression about the current take-up rate of cyber or data breach insurance policies.

According to the U.S. Census Bureau’s 2011 figures (the latest I could find on their website), there are about 5.7 million firms in the United States. To keep it simple, using six million firms for 2013 (which seems reasonable), then a 31% take-up rate means that
two million of them have cyber polices. The Financial Times cited to a June 2013 report from a risk consultant that estimated that the annual gross written premium for cyber polices was $1.3 billion. Doing some back of the envelope math means that the average annual premium for each of these two million cyber polices is $650. But according to the report prepared for Experian, of the 43% of respondents that have no plans to purchase a cyber policy, 52% cited premiums being too high as a reason. Not to mention that an average premium of $650—about what I pay per year for veterinary insurance for Barney my dog—seems low considering how hard many insurers are working to get a toe-hold on the cyber insurance market.

My sense is that, if 31% is the right number of companies that have a cyber policy, it is 31% of a certain type of company and not 31% of ALL U.S. companies across the board, as is being portrayed. Let’s take a look at the Experian report and how it arrived at 31%.

First, the Experian report—“Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age” (August 2013)—is really one that was independently prepared by Ponemon Institute LLC for Experian. According to the report, Ponemon is “dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.” For simplicity, I’ll refer to the Ponemon report as the Experian report.

How large was the sample size for the survey that was conducted to reach the 31% conclusion? Ponemon started with a random sample of 18,829 “experienced individuals involved in their companies’ cyber security risk mitigation and risk management activities in various-sized organizations in the United States.” 957 respondents completed the survey. After screening and reliability checks removed 319 surveys, the final sample was 638 surveys.

Of these 638 surveys, a whopping 86% were from companies with a global head count of 500 or more employees. Compare this with the percentage of all U.S. firms that have 500 or more employees, which is three-tenths of one percent according to the census folks. U.S. companies with fewer than twenty employees make up 90% of the total. Given the gargantuan difference between the size of the Experian companies, and U.S. companies in general, it is inconceivable that 31% of these very small companies—many probably just trying to make ends meet—have a cyber policy. Any comparison between these two groups is apples to washing machines.
The Ponemon survey asked if the respondent company, over the past 24 months, had experienced one or more cyber attacks that infiltrated the company’s networks or enterprise systems resulting in the loss or theft of 1,000 or more records. The number of respondents that answered yes was 56%. Of these companies, 60% pegged their out of pocket cost of the attacks at between $1 million and $25 million. So it is hardly a surprise that, of the companies that experienced a data breach, 70% said that such breach increased their interest in purchasing cyber insurance.

You do not need a degree from MIT to see that it is very hard to say that 31% of ALL U.S. companies have cyber policies, as the Experian report’s conclusion has been described. Not even close. The actual across the board number has to be many, many multiples fewer. All that can be said about the Experian report is that 31% of mostly the largest companies in the country, half of which have already experienced a data breach, have a cyber policy.

None of this is to say that there is anything wrong with the Experian report. Its conclusion, that 31% of huge companies, half of which have already been stung by a data breach, have a cyber policy, sounds entirely reasonable. The authors of the Experian report are quick to point out that there are limitations in it. Among other caveats, they state that “[t]here are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings.”

The problem with the Experian report is not its conclusion, but that such conclusion has been applied too broadly and then treated as if it were written on stone tablets. It reminds me of Y2K. Someone was the first to say that airplanes may fall out of the sky at the stroke of midnight on January 1, 2000. That possibility was then continuously repeated in article after article after article addressing the Year 2000 risks.

While the number of U.S. companies that have a cyber policy may be elusive, this much can be said with certainty. Based on the recent data breach at Target, and other widely-reported breaches, the number of policies can only go in one direction. The Target data breach was the equivalent of ten free Super Bowl ads for insurers selling cyber policies.

*   *   *

136
Increased Regulatory Focus on Cybersecurity Underscores Need for Public Companies to Review Cybersecurity-Related Disclosures

Yafit Cohn
Simpson, Thacher & Bartlett LLP

I. Recent Focus on Cybersecurity

As a result of recent highly publicized data breaches at a number of public companies, lawmakers and regulators have become increasingly focused on the issue of cybersecurity. Renewed attention on cybersecurity is evident, for example, in the various bills pending in Congress that address the issue, such as by seeking to require companies to implement certain data privacy and security standards and to notify customers of breaches within a specified time period. Additionally, in accordance with an executive order issued by President Obama, the National Institute of Standards and Technology recently released its “Framework for Improving Critical Infrastructure Cybersecurity,” which provides a set of voluntary “industry standards and best practices to help organizations manage cybersecurity risks.”

And Securities and Exchange Commission (“SEC”) Chairman Mary Jo White testified several months ago before the U.S. Senate Committee on Banking, Housing, and Urban Affairs that information security is among the 2014 examination priorities of the SEC’s National Exam Program.

In addition to increased emphasis on ensuring that companies safeguard personal data and effectively manage cybersecurity threats, recent interest in cybersecurity may mean heightened regulatory scrutiny of public companies’ disclosures on cybersecurity risks and threats in their filings with the SEC. Thus, it is crucial that public companies heed the advice of the SEC’s Division of Corporation Finance (the “Division”) to “review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents,” keeping in mind the Division’s 2011 guidance regarding cybersecurity disclosures.

II. Disclosure Guidance of the SEC’s Division of Corporation Finance

In 2011, when it issued its guidance, the Division recognized that while there is no disclosure requirement in the federal securities laws explicitly referring to cybersecurity, there are “specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.”

2 Mary Jo White, Testimony on “Oversight of Financial Stability and Data Security” before the United States Senate Committee on Banking, Housing, and Urban Affairs (Feb. 6, 2014).
4 Id.
1. Risk Factors: If the risk of cyber incidents is among “the most significant factors that make the offering speculative or risky,” a registrant must disclose it in its Risk Factors discussion.\(^5\) According to the Division, determining whether risk factor disclosure is required necessitates a registrant’s evaluation of its cybersecurity risks, taking into account all relevant information, including: “prior cyber incidents and the severity and frequency of those incidents”;

- “the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks”; and

- “the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry” in which the registrant operates, as well as risks to the registrant’s cybersecurity system (including threatened attacks).\(^6\)

As with other risk factors, a registrant’s disclosure must be tailored to its specific facts and circumstances – not “a generic ‘boilerplate’ disclosure” – and must adequately describe each material cybersecurity risk and explain how each risk affects the registrant.\(^7\) This may require disclosure of actual or threatened cyber incidents, as well as the known or potential costs or other consequences stemming from any such incident, to the extent they are material. A registrant need not, however, provide any disclosure that itself would compromise its cybersecurity.

2. Management’s Discussion and Analysis of Financial Condition and Results of Operations (“MD&A”): Pursuant to the Division’s guidance, a registrant should discuss cybersecurity risks or incidents in its MD&A “if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.”\(^8\) In its disclosure, the registrant should include the possible outcomes, if material, of known or potential cyber incidents, such as an increase

---

\(^5\) Regulation S-K, Item 503(c). As with other risks, a registrant should not “present risks that could apply to any issuer or any offering.” \(Id\); see also CF Disclosure Guidance: Topic No. 2, Cybersecurity.


\(^7\) \(Id\). According to the Division, “[d]epending on the registrant’s particular facts and circumstances, and to the extent material, appropriate disclosures may include: Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences; To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks; Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences; Risks related to cyber incidents that may remain undetected for an extended period; and Description of related insurance coverage.” \(Id\).

\(^8\) \(Id\).
in cybersecurity protection costs or a reasonable likelihood that the attack will result in reduced revenues.

3. Description of Business: According to the Division, if, upon evaluating the impact of cyber incidents on the registrant’s reportable segments, a registrant determines that the incidents “materially affect [the] registrant’s products, services, relationships with customers or suppliers, or competitive conditions,” the registrant should include a discussion of the incident and its potential material consequences in its Description of Business.

4. Legal Proceedings: If a registrant or one of its subsidiaries is a party to any material pending legal proceeding involving a cyber incident, information regarding the litigation may need to be disclosed in the registrant’s Legal Proceedings disclosure.

5. Financial Statement Disclosures: The Division advised registrants to ensure the proper accounting of costs attendant to cybersecurity and cyber incidents. For example, the Division directed registrants to consider accounting standards relevant to:

- Capitalization of costs incurred to prevent cybersecurity breaches, if such costs are related to internal-use software;
- Incentives provided to customers aimed at retaining their business following a cyber incident;
- Losses from asserted and unasserted claims, “including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts”; and
- Diminished future cash flows, “requiring consideration of impairment of certain assets.”

6. Disclosure Controls and Procedures: In evaluating whether its disclosure controls and procedures are effective, a registrant should consider, among other things, the extent to which any cyber incidents affect its “ability to record, process, summarize, and report information that is required to be disclosed in Commission filings.” If, for example, “it is reasonably possible that information would not be recorded properly

---

9 Id.
10 Id.
11 Id.
due to a cyber incident affecting a registrant’s information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.”12

III. SEC Comment Letters on Cybersecurity Disclosures

Since the Division issued its guidance two-and-a-half years ago, there has been a significant increase in SEC comment letters to registrants regarding their cybersecurity-related disclosures. In May of 2013, Chairman White indicated that since the publication of the Division’s guidance, the SEC’s staff “issued comments addressing cybersecurity matters to approximately 50 public companies of varying size and in a wide variety of industries.”13 The number of public companies receiving comments on these issues has further grown since then.

The SEC’s comments with regard to companies’ disclosures on cybersecurity risks and incidents generally fall into one of four categories:

1. Disclosures Silent About Cybersecurity Risks: Where a company’s disclosures do not reference cybersecurity risks, the SEC may request that the registrant provide appropriate risk factor disclosure regarding cybersecurity issues or may ask the registrant what consideration it gave to the Division’s guidance to address, among other things, (a) whether the registrant has been subject to any cybersecurity attacks, (b) the adequacy of preventative actions taken to decrease cybersecurity risks, (c) if applicable, the risks resulting from outsourcing of any functions that have material cybersecurity risks, (d) risks related to cyber incidents that may remain undetected for an extended period of time, and (e) whether the registrant has obtained relevant insurance coverage.

2. Disclosures Listing Cybersecurity Risks Among Other Potential Hazards: Where a company’s disclosures include cybersecurity risk in a list along with other potential catastrophic events, the SEC may request that in the future, the company provide a separate discussion of risks posed to its operations as a result of the company’s dependence on technology or to the company’s business, operations, or reputation by cyber attacks. The SEC may also remind the registrant to disclose any actual or attempted cyber attacks it has experienced, in order to put its risk factor disclosure in context.

3. General Cybersecurity Disclosures: Where a company’s filings provide generally that the company is subject to cybersecurity risks or that computer hacking or other network breaches may materially adversely affect its operations (e.g., “We are subject to

12 Id. In addition to discussing the potential applicability of specific disclosure requirements to cybersecurity risks and incidents, the Division reminded registrants that, as with other matters, “material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.” Id.

13 Letter from Chairman White to Senator John D. Rockefeller IV (May 1, 2013).
cybersecurity risks”), the SEC may ask the registrant what consideration it gave to the Division’s guidance (as in number 1, above) or may request that the registrant disclose any security breaches of cyber attacks it has experienced in the past, in order to provide proper context for its risk factor disclosure. In addition, where a company advises the SEC in the comment letter process that it has not experienced any security breaches or cyber attacks that had a material adverse effect on its operations, the SEC often requests that in future filings, the company disclose any cyber incidents that did not result in a material adverse effect on its operations, in order to ensure that investors are aware that the company is experiencing these risks.

4. Disclosures Regarding a Cybersecurity Incident: Where a company discloses a security breach, the SEC may request the disclosure of additional information, often in accordance with the Division’s guidance, such as the scope and magnitude of the breach, whether the incident was material, any known or potential costs resulting from the breach, or any preventative measures taken to reduce the risk of future cyber incidents.

IV. Conclusion

The SEC continues to actively examine registrants’ disclosures and consider disclosure requirements with regard to cybersecurity threats and incidents. In May of 2013, Chairman White noted that she has asked the SEC staff to brief her on public companies’ current disclosure practices and their overall compliance with the Division’s guidance and requested their recommendations for further action on the issue.14 On March 26, 2014, the SEC also held a roundtable “to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns,” including how public companies are disclosing cybersecurity threats and incidents.15

In the meantime, registrants should review their cybersecurity-related disclosures and consider their adequacy in light of the Division’s guidance. Robust disclosures in compliance with the Division’s advice may help prevent (or defeat) a shareholder class action or derivative lawsuit in the event of a data breach followed by a decline in stock price.

*    *    *

14 This request followed an April 9, 2013 letter from Senator John D. Rockefeller IV to Chairman White, opining that despite the Division’s guidance, cybersecurity disclosures “are generally still insufficient for investors to discern the true costs and benefits of companies’ cybersecurity practices” and urging the SEC to “elevate [the Division’s] guidance and issue it at the Commission level as well.”

California Court of Appeals Creates New Argument for Protecting Anonymous Online Speech

by Paul Alan Levy

Consumer Law & Policy Blog

In a decision issued today, the California Second District Court of Appeal has created an additional way for anonymous speakers, and for web operators who host anonymous comments, to protect the right to speak anonymously. Instead of invoking the First Amendment as courts in other states, and indeed other appellate courts in California have done, the Court of Appeal reversed an order compelling the identification of an anonymous speaker because the discovery order violated the state constitutional right of privacy.

The issue arose when Escape Media Group, in the course of fighting off a pair of lawsuits in which UMG Recordings charged that Escape’s Grooveshark music service infringes copyright, sent a subpoena to Digital Music News seeking to identify an anonymous commenter who posted a pair of comments to an article about Grooveshark; the commentere asserted that he was an Escape employee and charged that the reason why so many copyrighted recordings appear on Grooveshark without the consent of the copyright holders is that Escape creates financial incentives for employees to upload copyrighted recordings that are in high demand. Digital argued both that the First Amendment entitled the commenter to remain anonymous, and that the identifying data had been deleted in the ordinary course of business because Digital does not have any ongoing need for server logs.

The trial court enforced the subpoena after Escape provided an affidavit averring that the anonymous comments were false in several ways, and then allowed Escape to demand a forensic examination of Digital’s computer servers to determine whether the deleted data could be located in the unallocated blocks. Digital appealed, arguing both that the First Amendment barred the underlying discovery and that, in any event, a third party that has deleted data in the ordinary course of business before receiving a subpoena cannot be required to preserve its servers or open them up to forensic examination.

The Court of Appeal reversed in a unanimous opinion by Justice Victoria Gerrard Chaney, but not on either of these grounds. Instead, in light of the fact that, while the
appeal was pending, the New York Appellate Division struck Escape’s DMCA immunity defense on the ground that the DMCA protects only against federal infringement claims, not state law claims for infringement of pre-1972 sound recordings, the court decided that the discovery was not relevant to the state court infringement action, however relevant it might have been had the subpoena been issued in the federal law infringement action.

The court went on the say, however, that even if the subpoena met the ordinary test of relevance, discovery to identify an anonymous speaker implicates the speaker’s right of privacy under the California constitution. Consequently, the court had to apply a multi-factor test that requires consideration of the extent to which the party has “a compelling need for discovery,” and whether that need is so strong as to “so strong as to outweigh the privacy right when these two competing interests are carefully balanced.” In this regard, the court took into consideration not just Escape’s minimal need for discovery, but also the problem that, if the anonymous commenter really was an Escape employee, “exposure could endanger not only his or her privacy but also livelihood.” In this regard, the privacy approach might provide even stronger protection that the approach taken under the First Amendment by the Sixth District Court of Appeal in northern California, which held in Krinsky v. Doe that once a plaintiff shows that an anonymous comment is a false statement of fact that caused damage, no balancing of the interests of the interests is required as in the majority approach representing by the Dendrite line of analysis.

The Court closed with a paragraph that more judges might heed, whether they are weighing anonymity in a First Amendment or right of privacy context. Indeed, litigants might also entertain this thought before filing a lawsuit or serving a subpoena:

Visitor has done nothing more than provide commentary about an ongoing public dispute in a forum that could hardly be more obscure—the busy online comments section of a digital trade newspaper. Such commentary has become ubiquitous on the Internet and is widely perceived to carry no indicium of reliability and little weight. We will not lightly lend the subpoena power of the courts to prove, in essence, that Someone Is Wrong On The Internet.

* * *

143
UNITED STATES COURT OF APPEALS  
FOR THE FIRST CIRCUIT  

Nos. 12-1835  
12-1858  

UNITED STATES OF AMERICA,  
Appellee,  

v.  

TODD LYONS  
and DANIEL EREMIAN,  

Defendants, Appellants.  

APPEALS FROM THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS  

[Hon. Patti B. Saris, U.S. District Judge]  

Before  

Lynch, Chief Judge,  
Thompson and Kayatta, Circuit Judges.  

Peter Charles Horstmann, with whom Partridge, Ankner & Horstmann, LLP was on brief, for appellant Todd Lyons.  
Juan Chardiet, with whom Chardiet Law P.C. was on brief, for appellant Daniel Eremian.  
John M. Pellettieri, Attorney, Appellate Section, Criminal Division, U.S. Department of Justice, with whom Mythili Raman, Acting Assistant Attorney General, Denis J. McInerney, Acting Deputy Assistant Attorney General, Carmen M. Ortiz, United States Attorney, and Robert A. Fisher, Mary Beth Murrane, and Fred W. Wyshak, Assistant U.S. Attorneys, were on brief, for appellee.  

January 17, 2014
KAYATTA, Circuit Judge. Todd Lyons and Daniel Eremian worked for Sports Off Shore (SOS), a gambling business based in Antigua. After a wide-ranging investigation by federal and state law enforcement of SOS and its employees and agents, and a lengthy trial, a jury convicted both Lyons and Eremian on two counts under the Wire Act, 18 U.S.C. § 1084, two counts under RICO, 18 U.S.C. §§ 1962(c) and 1962(d), and one count under 18 U.S.C. § 1955 for conducting an illegal gambling business. Lyons was separately convicted on another eighteen counts. In this direct appeal from their convictions and sentences, Lyons and Eremian argue that: (1) the district court improperly denied them a safe harbor instruction on the government's charges that they violated the Wire Act; (2) the Wire Act does not apply to the internet; (3) the government did not prove they had the necessary mens rea to violate the Wire Act; (4) their convictions involved an inappropriate extraterritorial application of the Wire Act; (5) their Wire Act convictions should be overturned because the government was required but failed to prove that all relevant bets were on sporting events; and (6) the district court improperly admitted into evidence a directory of SOS agents.

Lyons separately argues that: (7) the district court should have suppressed evidence derived from wiretaps of his phone conversations; (8) the district court should have suppressed evidence obtained pursuant to search warrants for his home, car,
and person; (9) there was insufficient evidence to convict him of money laundering because the government's evidence did not distinguish between "proceeds" and "profits" of illegal gambling; (10) there was insufficient evidence to convict him of violating the Travel Act, 18 U.S.C. § 1952, for the same reason; (11) the absence of final implementing regulations precluded his convictions for violating the Unlawful Internet Gambling Enforcement Act of 2006 ("UIGEA"), 31 U.S.C. §§ 5361-67; and (12) the prosecution referred at trial to his decision not to testify, violating his Fifth Amendment right against self-incrimination.

Eremian separately argues that: (13) venue did not lie in Massachusetts; (14) there was insufficient evidence to convict him of racketeering; and (15) instructing the jury on Florida law constituted a constructive amendment of the indictment. Finally, Lyons and Eremian each challenges his punishment, arguing that (16) his prison sentence and the forfeiture judgment were unreasonable and violated the Eighth Amendment.

In the remainder of this opinion, we address these sixteen arguments in the order listed, above. For the reasons stated, we affirm the convictions and sentences, though we affirm Lyons's Wire Act convictions in one limited respect on a basis different from that employed by the district court.
I. Background

SOS was a bookmaking business founded in 1996 by Robert Eremian, Daniel Eremian's brother.¹ SOS centered its operations in Antigua at least in part because some forms of bookmaking are legal there. Many of SOS's customers, however, were in the U.S. and SOS took bets by phone or over the internet from the U.S. Most SOS customers bet on team sports, but others bet on horse racing or on casino games played on the SOS website. SOS allowed bettors to place bets against funds placed on deposit with SOS, or on credit. Antiguan regulatory law allowed the former but, at least between 2001 and 2007, prohibited betting on credit.

A bettor who wished to place bets on credit with SOS received a password and a customer code for placing bets through the internet or by phone. SOS employed agents in the United States, including Eremian and Todd Lyons, to "settle up" with credit bettors, collecting losses from losers and making payments to winners. These agents met with bettors in person in public places and primarily conducted transactions in cash or by receiving checks. Each agent managed a group of regular customers and received as a commission a percentage of those customers' losses. Some agents also employed sub-agents who managed their own

¹ This opinion will always refer to Robert Eremian by his full name. "Eremian," on its own, will be used to refer to Daniel Eremian.
customers and shared commissions with the agents under whom they worked.

After deducting their commissions from the money leftover once customers settled up, the agents sent the balance to SOS in Antigua. Agents often sent this balance in cash, sometimes using a "six pack," a package containing three bundles of $2,000. SOS agents also carried cash to Antigua in person. Agents also transferred or caused their customers to transfer funds to Antigua by check or wire transfer.

Daniel Eremian played an important role in the SOS operation from its inception. He helped his brother establish the SOS office in Antigua, training Antiguan employees about how to answer the phone and take bets. After SOS was established, Eremian returned to the United States where he worked as an SOS agent. He recruited customers in Florida. He also employed at least three sub-agents. Like other SOS agents, Eremian provided bettors with the information needed to place bets with SOS on credit and settled up with customers, either in-person or through his sub-agents. On at least one occasion, Eremian also collected funds from another agent on behalf of SOS.

Todd Lyons came to SOS later than Eremian, but ended up playing a larger role in SOS's Massachusetts operation than Eremian played in Florida. Like many agents, Lyons was a bettor with SOS before he became an agent. But at some point between 1997 and 2000
Lyons became an SOS agent. Like other SOS agents, Lyons provided customers with the information they needed to make bets. He also collected losses and distributed winnings. Lyons had at least one sub-agent. In addition to working as an agent, Lyons also served as "the bank" for SOS in Massachusetts, collecting money from, and disbursing it to, other agents. Starting in 2000, SOS paid Lyons a salary for this managerial role.

Lyons first drew the attention of Massachusetts state police investigating an illegal bookmaker in Boston. Police and prosecutors sought and received a wiretap of Lyons's cell phone. This wiretap led to warrants for searches of Lyons's home, car, and person conducted in January, 2006. The search of Lyons's home uncovered records of bets and cash disbursements, and a substantial quantity of cash, including $34,318 in a briefcase and $50,000 in the leg of a pair of pants in a drawer. The Massachusetts State Police continued to investigate Lyons until 2009, when they executed a second search warrant for his house, finding $93,800 hidden above two ceiling tiles and more gambling records. A federal grand jury indicted Lyons in May, 2010. A superseding indictment was filed in August, 2010, charging Daniel Eremian, Robert Eremian, Lyons, and Richard Sullivan, another important figure in SOS. As of March 1, 2012, Robert Eremian and Sullivan were fugitives.
II. Analysis

We first address Lyons's and Eremian's common challenges to their convictions, then their individual challenges to their convictions, and finally their challenges to their sentences.

1. The Safe Harbor Provision of the Wire Act

Both Lyons and Eremian were convicted on two counts of violating the Wire Act by transmitting bets or betting information or assisting the transmission of bets over a wire communication facility. One count charged them with violating the Wire Act using telephones, the other with violating the Wire Act using the internet. In a challenge directed at both counts, they argue that the district court erred by failing to instruct the jury on the safe harbor provision of the Wire Act, 18 U.S.C. § 1084(b), which exempts from liability certain communications assisting in the transmission of bets between places where betting on sports is legal.

We review preserved claims of instructional error de novo. United States v. Baird, 712 F.3d 623, 627-28 (1st Cir. 2013). If this de novo review concludes that "the evidence at trial, taken in the defendant's favor, was sufficient to support his requested instruction, then we move to a three-part test to decide whether the district court's refusal to give the instruction constitutes reversible error." Id at 628. Reversal is only appropriate if the requested instruction was "(1) substantively
correct as a matter of law, (2) not substantially covered by the charge as rendered, and (3) integral to an important point in the case so that the omission of the instruction seriously impaired the defendant's ability to present his defense."  Id.

For the following reasons, we find that Eremian was not entitled to an instruction on the safe harbor provision, and that it makes no difference whether Lyons was entitled to such an instruction.

a. Statutory Background

The Wire Act has two provisions relevant to Lyons and Eremian. Section 1084(a) creates criminal liability:

Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.

Section 1084(b) creates an exception to section 1084(a) applicable to certain transmissions of information assisting in the placing of bets:

Nothing in this section shall be construed to prevent . . . the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State or foreign country where betting on that sporting event or contest is legal into a State or foreign country in which such betting is legal.
Two aspects of this safe harbor provision are pertinent to our analysis in this case. First, the safe harbor provision only applies when gambling on the events in question is legal in both the sending and receiving jurisdiction. Thus, for example, if New York allows betting on horses at race tracks in New York, and if Nevada allows betting in Nevada on the results of New York horse races, then information may be wired from New York to Nevada to assist in the betting in Nevada without violating the statute. See H.R. Rep. No. 87-967, reprinted in 1961 U.S.C.C.A.N. 2631, 2632-33. Second, the safe harbor provision only applies to the transmission of "information assisting in the placing of bets." The safe harbor provision does not exempt from liability the interstate transmission of bets themselves. See United States v. McDonough, 835 F.2d 1103, 1104-05 (5th Cir. 1988); United States v. Bala, 489 F.3d 334, 342 (8th Cir. 2007).

In this manner, the Wire Act prohibits interstate gambling without criminalizing lawful intrastate gambling or prohibiting the transmission of data needed to enable intrastate gambling on events held in other states if gambling in both states on such events is lawful.

b. Applying Section 1084(b) to Lyons and Eremian

Lyons and Eremian sought protection under section 1084(b)'s safe harbor provision in two ways: they argued that they were entitled to an acquittal as a matter of law because
all of their charged Wire Act violations fell within the safe harbor provision; and they argued in the alternative that, at the very least, the district court should have instructed the jury on the safe harbor provision because some of their activities fell within it.

Eremian's effort to rely on the safe harbor provision in this manner is a non-starter. Many transmissions he caused were from Florida. He advances no argument that the bets made by SOS bettors in Florida were legal in Florida. Nor could he. See Fla. Stat. § 849.14. Simply put, there was no evidence at all to support his argument that the safe harbor provision could apply to him and therefore no error in denying him an instruction on it. Cf. Baird, 712 F.3d at 627. A fortiori, it follows that the safe harbor did not render insufficient the evidence marshaled against him.

Lyons had a better potential argument regarding the safe harbor because it is not clear that either Massachusetts or Antigua makes sports betting illegal. Both Massachusetts and Antigua law place limits on gambling, but otherwise allow it. Antigua appears to generally allow bets on sporting events, although bets may not be placed on credit. Massachusetts law criminalizes betting by telephone. Mass. Gen. Laws ch. 271, § 17A. It also criminalizes the operation and patronizing of gaming houses, id. at § 5, and the manufacture and sale of gaming devices. Id. at § 5A. The
government, though, points to no Massachusetts law effectively criminalizing betting on sporting events generally. The government nevertheless argues that the bets placed from Massachusetts to Antigua cannot be within the safe harbor provision because they violated the Antiguan gaming regulations. Lyons counters that a bet is "legal" for the purposes of the Wire Act as long as "betting on that sporting event . . . is legal," 18 U.S.C. § 1084(b), in the jurisdiction. Cf. Bala, 489 F.3d at 341-42 (8th Cir. 2007) (holding that non-compliance with statutory requirement that parimutuel betting businesses donate a portion of their proceeds to charity did not mean that betting at those business was "illegal" for purposes of section 1084(b)). But cf. United States v. Cohen, 260 F.3d 68, 73-74 (2d Cir. 2001) (holding that sports betting was "illegal" under section 1084(b) where it was not a crime but was generally prohibited by law and the state constitution).

We need not resolve this dispute. Specifically, in Lyons's case, we need not decide if some of the activity for which he was indicted fell within the safe harbor. Rather, because the evidence was overwhelming that he also engaged in other activity clearly outside the safe harbor, for which he was indicted under the same count, his arguments based on the safe harbor must fail. Where a jury is properly instructed on two theories of guilt, one of which is later determined to be invalid, "we can affirm the conviction only if we conclude 'beyond a reasonable doubt' that
'the jury verdict would have been the same absent the error.'"

United States v. Zhen Zhou Wu, 711 F.3d 1, 30 (1st Cir. 2013) (quoting Neder v. United States, 527 U.S. 1, 17 (1999)). Here, given the overwhelming evidence of Lyons's guilt under an aiding and abetting theory, the district court's refusal to instruct the jury on the safe harbor defense arguably applicable to some of Lyons's acts provides no cause for reversal. A fortiori, his sufficiency argument based on the safe harbor must similarly fail.

The indictment on the two Wire Act counts charged Lyons not just with transmitting information assisting in the placing of bets, but also with aiding and abetting the use of a wire communication facility for the transmission of bets. It alleged that "Eremian . . . Lyons, and others unknown to the grand jury, each aiding and abetting the other, being engaged in the business of betting and wagering, knowingly used a wire communication facility for the transmission in interstate and foreign commerce of bets and wagers . . . on any sporting event or contest." Receiving bets is "use" of a wire communication facility. See Sagansky v. United States, 358 F.2d 195, 200 (1st Cir. 1966). Under 18 U.S.C. § 2(a) "[w]hoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal." Therefore, if Lyons aided and abetted the receipt of bets by SOS he falls outside the protection of the safe harbor provision.
An aider and abettor is punishable as a principal if, first, someone else actually committed the offense and, second, the aider and abettor "became associated with the endeavor and took part in it, intending to ensure its success." United States v. Spinney, 65 F.3d 231, 235 (1st Cir. 1995). "The central requirement of the second element is 'a showing that the defendant consciously shared the principal's knowledge of the underlying criminal act, and intended to help the principal.'" Id. (quoting United States v. Taylor, 54 F.3d 967, 975 (1st Cir. 1995)). Lyons was not required to know the exact details of each individual transaction to be liable as an aider and abettor—it is sufficient that he knew of SOS's receipt of bets and knowingly helped it continue to receive them. See United States v. Davis, 717 F.3d 28, 33 (1st Cir. 2013) ("[A] culpable aider and abettor need not perform the subject offense, be present when it is performed, or be aware of the details of its execution." (internal quotation marks omitted)); United States v. Hernandez, 218 F.3d 58, 65 (1st Cir. 2000) (knowledge of all details of a drug transaction not needed for aiding and abetting liability).

Any reasonable jury would necessarily have found beyond a reasonable doubt that Lyons aided and abetted SOS's receipt of inter-jurisdictional bets. The core mission of SOS was to engage in the business of interstate gambling on, among other things, sporting events, by causing and receiving the interstate and

-13-
foreign transmission of wagers. It could not do this without receiving bets. Lyons's efforts for over a decade were dedicated to facilitating that business. Lyons handled millions of dollars in proceeds from SOS agents in Massachusetts. He functioned as SOS's "bank" in the state, collecting bettors' losses, distributing winnings, and collecting money from and distributing it to SOS agents. SOS paid him a salary for this role. SOS would have received no bets had it lacked a way to settle up with bettors and so Lyons' role was critical to its receipt of bets.

Like other agents Lyons also aided and abetted the receipt of bets by SOS by functioning as an agent. Witnesses described Lyons as the agent who provided them with the information they needed to place bets with SOS, collected losses from them, and distributed winnings. He also specifically directed at least one bettor to make payments to SOS by wire transfer to settle up bets placed with SOS. Perhaps the best evidence that Lyons intended to ensure SOS's success by these actions, besides the actions themselves, is that he received a commission of 50 percent of the losses of the bettors he personally managed. Lyons was a critical part of SOS's operation and thereby demonstrated a clear intent to further SOS's business of receiving illegal inter-jurisdictional sports bets by phone and over the internet.

Nor could Lyons avoid liability for aiding and abetting the commission of a crime even if he could show that some of the
charged conduct could have been performed lawfully. It is perfectly legal to drive a friend to the bank, but doing so with an intent to help him rob it is a crime. See Spinney, 65 F.3d at 235 (1st Cir. 1995). Similarly, accompanying a friend to a business meeting is not a crime, but doing so with an intent to further the sale of cocaine is. See United States v. Paone, 758 F.2d 774, 776 (1st Cir. 1985). And while working as a crewman on a boat is legal, doing so with an intent to aid its transportation of marijuana is not. See United States v. Cuevas-Esquivel, 905 F.2d 510, 515 (1st Cir. 1990). Many of Lyons's actions, moreover, violated other criminal statutes as the other counts he was convicted of show, and so this is not even a situation in which aiding and abetting liability transforms otherwise purely lawful conduct into criminal action. The two specific payments to SOS Lyons was convicted of causing, for example, formed the basis of Lyons's money laundering conviction we affirm below. Given the clear evidence of Lyons's intent to further SOS's receipt of bets in violation of the Wire Act we therefore have no trouble affirming his conviction on this basis.

2. The Internet and the Wire Act

Lyons and Eremian argue for the first time on appeal that they should have been granted an acquittal as a matter of law on the Wire Act count that was based on the transmission of information over the internet because, they claim, the internet is
not a "wire communication facility." They did not raise this specific argument in their post-trial motion for acquittal, in which they objected generally to the sufficiency of the evidence, but also made certain other specific objections. Normally, a general objection to the sufficiency of the evidence preserves all possible sufficiency arguments, but we have also suggested that a defendant who raises only specific sufficiency arguments waives all those he does not make. See United States v. Marston, 694 F.3d 131, 134 (1st Cir. 2012) (collecting cases for both propositions). We have not decided what happens when a general sufficiency objection is accompanied by specific objections, but we have suggested, albeit in dictum, that such a practice preserves all possible objections because: "[i]t is helpful to the trial judge to have specific concerns explained even where a general motion is made; and to penalize the giving of examples, which might be understood as abandoning all other grounds, discourages defense counsel from doing so and also creates a trap for the unwary defense lawyer." Id. at 135. We need not decide the issue, however, because, whatever the standard of review, the sufficiency challenge fails.

The sufficiency challenge fails because the internet is an "instrumentalit[y] . . . used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and
reception of such transmission." 18 U.S.C. § 1081; see also United States v. Cohen 260 F.3d 68, 76 (2d Cir. 2001) (transmitting bets over the internet violated the statute because it involved transmission to and from customers of betting information). Anyone reading this opinion on the court's website or the like would readily agree that the internet is used and useful in the transmission of writings. Indeed, it is rather remarkable that a definition written before the internet was invented so accurately describes it. When, as here, the text of a statute "provides a clear answer" to a question of statutory construction our "inquiry ends." United States v. Robinson, 459 F.3d 39, 51 (1st Cir. 2006).

The Wire Act's evident applicability to the internet likewise means that its application to Lyons and Eremian is not, contrary to their claims, an impermissible ex post facto "novel construction of a criminal statute to conduct that . . . the statute . . . has [not] fairly disclosed to be within its scope." United States v. Lanier, 520 U.S. 259, 266 (1997).

The argument to the contrary relies on two misapprehensions: First, that the Wire Act cannot be applied to communications over the internet because the Act was enacted in 1961, before the internet was created and, second, that because the internet is in some manner structurally dissimilar to a telephone or telegraph system, the Wire Act cannot apply to it. On the first point, we regularly apply statutes to technologies that were not in
place when the statutes were enacted. See, e.g., Sec. & Exch. Comm'n v. SG Ltd., 265 F.3d 42, 55 (1st Cir. 2001) (Securities Act of 1933 and Securities Act of 1934 applied to virtual shares which exist only in online game); United States v. Nichols, 820 F.2d 508, 511 (1st Cir. 1987) (theft statute applied to theft of information from computer network). As for the second point, nothing in the statute suggests that any instrumentality covered by the Wire Act must be structurally similar to a telephone exchange.

Nor is it relevant that the internet is not a common carrier, as Lyons and Eremian argue. While section 1084(d) does impose certain requirements on common carriers who are informed their facilities are being used for gambling, nothing in section 1084 or section 1081 limits the application of the Wire Act to transmissions made via common carriers.2

2 Lyons and Eremian also argue that "[r]epeated unsuccessful efforts by the [sic] Congress to amend the Wire Act are further evidence that it does not apply to Internet-gambling of whatever type." Even if unsuccessful attempts to amend a statute decades after it was passed were relevant to our interpretation of that statute, which we doubt, Lyons and Eremian point only to evidence that Congress sought to amend the Wire Act to criminalize forms of gambling other than sports betting. See In re MasterCard Int'l Inc., Internet Gambling Litig., 132 F. Supp. 2d 468, 480 (E.D. La. 2001) aff'd sub nom In re MasterCard Int'l Inc., 313 F.3d 257 (5th Cir. 2002). Elsewhere, Lyons and Eremian suggest that the passage of UIGEA suggests that Congress felt that the Wire Act did not apply to the internet either because it felt the need to pass legislation particularly targeting internet gambling or because "Congress could have used this occasion to amend/modernize the Wire Act to specifically include the Internet" but declined to do so. However, Congress made clear when it passed UIGEA that it did not modify existing gambling laws. 31 U.S.C. § 5361(b).
3. Mens Rea and the Wire Act

Lyons and Eremian also argue that the government did not prove they had the necessary mens rea to violate the Wire Act. What exactly they say the government failed to prove is unclear. Reading their pleading generously, they appear to argue that even if the internet is a wire communication facility as a matter of law, the government was required to prove that they knew the law. While there are certainly good reasons why Congress might not wish to punish as criminals persons who do not know their conduct may be unlawful, as a general matter ignorance of the law is no defense. See Bryan v. United States, 524 U.S. 184, 193 (1998) ("[U]nless the text of the statute dictates a different result, the term 'knowingly' merely requires proof of knowledge of the facts that constitute the offense." (footnote omitted)); United States v. Cohen, 260 F.3d 68, 76 (2d Cir. 2001) (In proving mens rea under the Wire Act, it "mattered only that [the defendant] knowingly committed the deeds forbidden by § 1084, not that he intended to violate the statute."). Moreover, it is widely known that many forms and means of gambling are regulated or prohibited. Certainly, persons engaged in wide-ranging gambling operations and storing large sums of cash in socks, ceilings, and "six-packs" are not engaged in the types of conduct that would justify applying any exception to the general rule that ignorance of the law is no excuse.
4. Extraterritoriality and the Wire Act

Lyons's and Eremian's convictions were not an improper extraterritorial application of the Wire Act. It is a "longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." Equal Opportunity Emp't Comm'n v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991) (internal quotation marks omitted), superseded in part by statute, see Arbaugh v. Y&H Corp, 546 U.S. 500, 512 n.8 (2006). The Wire Act expresses such a contrary intent because it explicitly applies to transmissions between the United States and a foreign country. 18 U.S.C. § 1084; cf. Pasquantino v. United States, 544 U.S. 349, 371-72 (2005) (stating that "the wire fraud statute punishes frauds executed in 'interstate or foreign commerce,'" and therefore can be applied extraterritorially because Congress did not have "only 'domestic concerns in mind.'" (quoting 18 U.S.C. § 1343 and Small v. United States, 544 U.S. 385, 388 (2005))). The communications giving rise to these convictions had at least one participant inside the United States and therefore fall within the statute's scope.

5. Proof of Sports Betting under the Wire Act

The Wire Act applies only to "wagers on any sporting event or contest," that is, sports betting. 18 U.S.C. 1084(a); see also In re MasterCard Int'l Inc., 313 F.3d 257, 263 (5th Cir.
Therefore, Lyons and Eremian say, there was insufficient evidence to convict them because some evidence at trial showed that SOS also accepted bets on casino games and other forms of gambling not covered by the Wire Act. But nothing in the statute limits its reach to entities devoted exclusively to sports betting any more than a bank robber gets off if he also withdraws money properly from an ATM. The district court instructed the jury that the Wire Act only applied to sports betting. And there was amply sufficient evidence that Lyons and Eremian, at least, aided and abetted the receipt of sports bets. SOS was, after all, "Sports Off Shore," not "Slots Off Shore." It advertised itself as a place to bet on sports, it published odds for sports bets, and its customer-witnesses testified that they placed bets on sports and paid their losses to Lyons and Eremian.

6. The Evidentiary Challenge to a Purported Directory of SOS Customers

At trial, Lyons and Eremian unsuccessfully objected to the government's introduction of a directory of SOS customers and agents. We review preserved evidentiary claims for abuse of discretion. See United States v. Rivera-Donate, 682 F.3d 120, 131 (1st Cir. 2012). After initially admitting the directory but reserving judgment on whether it could be admitted for the truth of the matter asserted, the district court later determined that it could be so admitted under Federal Rule of Evidence 801(d)(2)(E), which covers statements of a defendant's coconspirators.
Statements can only be admitted under Rule 801(d)(2)(E) if the district court finds by a preponderance of the evidence "(1) the existence of a conspiracy, (2) the defendant's membership in that conspiracy, (3) the declarant's membership in the same conspiracy, and (4) that the statement be made in furtherance of the conspiracy." Rivera-Donate, 682 F.3d at 131. The district court made such a finding.3

There is more than enough evidence in the record to conclude that the district court did not abuse its discretion by admitting the directory. Each page of the exhibit is titled "agent directory" and has the names and addresses of bettors along with a column labeled "limit" which contains numbers between 0 and 15,000. The directory was turned over to police by government witness Linda Richardson. Richardson testified that she helped her "lover and best friend, mostly best friend" Richard Sullivan, who was named in the indictment but is currently a fugitive, transfer and store money related to SOS. She found the directory within SOS business records Sullivan left in her possession, but testified that she had no prior knowledge that it existed. She recognized at least one

3 Lyons and Eremian claim that the directory was admitted under Federal Rule of Evidence 803(6)(B) but in fact the district court's references to United States v. Petrozziello, 548 F.2d 20, 23 (1st Cir. 1977), and to finding evidence of a conspiracy show that the court understood the evidence to be introduced under Rule 801(d)(2)(E). Indeed, Petrozziello actually represents a rule for the admission of evidence under Rule 802(d)(2)(E) which is narrower than that currently in effect. See United States v. Goldberg, 105 F.3d 770, 775-76 (1st Cir. 1997).
name on it as someone who had given or received a check to or from Richard Sullivan. The ledger also contained names and addresses for Daniel Eremian and Todd Lyons. Several other witnesses identified names on the list as SOS customers or agents, and some clarified that the agent number on the top of each page represented an SOS agent while the other names on that page were his customers.

Records that can be shown by a preponderance of the evidence to have been made by a member of a conspiracy may be admitted under Rule 801(d)(2)(E) even if their precise author cannot be identified. See, e.g., United States v. De Gudino, 722 F.2d 1351, 1355 (7th Cir. 1983); United States v. Smith, 893 F.2d 1573, 1577-78 (9th Cir. 1990); cf. United States v. Alosa, 14 F.3d 693, 697 (1st Cir. 1994) (records of a conspiracy admissible where "the district court expressly found by a preponderance of the evidence that the ledgers were made by conspirators in furtherance of the conspiracy."). Here, there was strong evidence that the directory was authored by Richard Sullivan or someone else involved with SOS because it contained information that would only have been available to someone in the illegal gambling conspiracy that was SOS and would have only been of use to someone managing SOS agents. And the record well supported the finding that Lyons and Eremian were members of that same conspiracy.

Lyons and Eremian also argue that, even if admission of the directory was correct under the Federal Rules of Evidence, it
nonetheless violated the Sixth Amendment's Confrontation Clause. But they misunderstand the Confrontation Clause, mistakenly believing it confers a general right to cross-examine the source of all evidence introduced at trial. Instead, the Confrontation Clause applies only to testimonial evidence; that is, evidence produced with a "primary purpose of creating an out-of-court substitute for trial testimony." *Michigan v. Bryant*, 131 S. Ct. 1143, 1155 (2011). For this reason, "[b]usiness and public records are generally admissible absent confrontation . . . because--having been created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial--they are not testimonial." *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 324 (2009). For the same reason, the directory was not testimonial.

7. The Lyons Wiretaps

The initial wiretap application targeted a phone used by a member of another gambling operation and was filed on October 12, 2005. After that application was approved, assistant district attorneys filed a series of renewal applications that expanded the initial authorization to include additional telephone numbers, including, on December 8, 2005, Lyons's number. Lyons was recorded both on his own phone and on others' phones. Before trial, Lyons moved to suppress evidence derived from all of these wiretaps.
While Lyons's brief conflates several distinct legal issues in its discussion of the wiretaps, he essentially makes three arguments: First, that the district court's decision that gambling is legal in Massachusetts means the wiretap applications were not supported by probable cause and the evidence derived from them should therefore be suppressed. Second, that the wiretaps were not authorized by the Essex County District Attorney and therefore were granted in violation of federal law and should be suppressed or at least should have been subject to challenge in an evidentiary hearing. Third, that even if the wiretaps were in fact authorized they should be suppressed because the initial wiretap application did not facially demonstrate that it was properly authorized. We address these arguments in turn.

a. Probable Cause for the Wiretaps

Lyons argues for the first time on appeal that the police lacked probable cause for the wiretaps. "A party waives [a suppression argument under rule 12(c)] . . . not raised by the deadline the court sets." Fed. R. Crim. P. 12(e). Here, Lyons did not raise this argument at all below. While "[f]or good cause, the court may grant relief from the waiver," id., Lyons has not addressed the waiver issue at all, let alone explained why he has good cause to seek relief from it. Despite Rule 12's clarity, we have suggested in the past that we may sometimes nonetheless review unpreserved suppression claims for plain error. See United States
v. Nuñez, 19 F.3d 719, 723 n.10 (1st Cir. 1994) (noting that some courts have conducted plain error review of claims waived under what was then Rule 12(f) and is now Rule 12(e), but also that this is not necessarily required). More recently, however, we have emphasized the categorical language of Rule 12(e) and made clear that it is "manifestly unfair" to the prosecution to allow the defendant to raise on appeal a suppression claim that was not raised below, even if suppression of the same evidence was sought on other grounds. United States v. Crooker, 688 F.3d 1, 9 (1st Cir. 2012) (quoting United States v. Walker, 665 F.3d 212, 228 (1st Cir. 2011)). We see no reason to find that manifest unfairness absent here.

b. Authorization of the Wiretaps

Lyons did timely raise in the district court his other two challenges to the wiretaps. The standard of review for preserved suppression arguments can be somewhat confusing because such motions interweave questions of fact and law:

When reviewing a challenge to a district court's decision on a suppression motion, we review the district court's factual findings and credibility determinations only for clear error. United States v. Camacho, 661 F.3d 718, 723 (1st Cir. 2011); see Ornelas [v. United States, 517 U.S. [690,] 699 . . . [(1996)] (findings of historical fact reviewed for clear error). We review the court's legal conclusions de novo. United States v. Rabbia, 699 F.3d 85, 89 (1st Cir. 2012). That being said, it is also true that we 'give due weight to inferences drawn from historical facts by resident judges and local law enforcement officers.' Ornelas, 517 U.S. at 699 . . . . As explained in United States v. Townsend, 305 F.3d 537 (6th Cir. 2002), the district court, which observes the
testimony of the witnesses and understands local conditions, is at an institutional advantage in making this determination. Id. at 542. "Accordingly, 'due weight' should be given to the inferences drawn from the facts by 'resident judges.'" Id. (quoting Ornelas, 517 U.S. at 698).

United States v. Dapolito, 713 F.3d 141, 147 (1st Cir. 2013).

Lyons's first preserved argument is that the wiretap applications were not reviewed by the Essex County District Attorney and are therefore invalid. Lyons is correct that a wiretap sought by state law enforcement must be authorized by the principal prosecuting attorney for the jurisdiction--either the state attorney general or the county district attorney, in this case the Essex County District Attorney. 18 U.S.C. § 2516(2). Under Massachusetts law, the principal prosecuting attorney need not himself appear in court in support of every wiretap application. Instead, he may specially designate a subordinate to exercise his authority on a case by case basis, but only in writing and after he has personally reviewed the wiretap application. Mass. Gen. Laws. ch. 272, § 99(F)(1); see also United States v. Smith, 726 F.2d 852, 857-58 (1st Cir. 1984) (citing Commonwealth v. Vitello, 367 Mass. 224 (1975)).

The Essex County District Attorney, Jonathan Blodgett, signed letters authorizing two assistant district attorneys to file
the first wiretap application at issue here. One letter was addressed to the state justice receiving the application and the other was addressed to the assistant district attorneys being specially designated. In addition to authorizing the assistant district attorneys to file the applications, the letter to the state justice explained that "all of [the wiretap applications] shall be reviewed by me or my designee before being presented to you."

Standing on its own, this letter might be insufficient because Massachusetts requires that the district attorney personally review the application—a designee is insufficient. Vitello, 367 Mass. at 231-32. However, in an initial ruling on the suppression motion, the district court determined that "[t]he fact that the designation letter, the letter to [the state justice], and the warrant application were all dated October 12 supports the reasonable inference that they were all presented together and that D.A. Blodgett was familiar with the contents of the application." This inference was not clearly erroneous. The district court therefore properly denied the suppression motion as to the phone numbers listed in the October 12th application.

---

4 The actual warrant applications are not part of the record on appeal or available on the district court docket. There is no dispute, however, that the initial wiretap at issue was sought by the assistant district attorneys designated by District Attorney Blodgett and so nothing in the wiretap applications is relevant to the issue before us.
Because the district court was uncertain whether Massachusetts law required re-designation and personal review by the district attorney when new numbers were added to an existing wiretap, it ordered District Attorney Blodgett to file "an affidavit regarding his authorization of the particular amendments at issue . . . ." District Attorney Blodgett filed such an affidavit in which he made clear that he "personally reviewed each and every renewal application" prior to its submission and that he intended the specially designated assistant district attorneys to oversee the entire investigation, including both the original wiretaps and the "renewals." The affidavit also stated that, as the district court inferred in its initial ruling, District Attorney Blodgett did in fact personally authorize the October 12th wiretap application. The district court therefore denied the suppression motion as to the remaining wiretaps.

We have previously held that, in combination with letters substantially equivalent to the ones that accompanied the initial application in this case, an affidavit like that submitted by District Attorney Blodgett is sufficient to establish actual authorization. United States v. Albertelli, 687 F.3d 439, 443 (1st Cir. 2012). We therefore have no reason to question the district court's factual finding that each wiretap application was specifically and personally authorized by District Attorney Blodgett as Massachusetts and federal law require. The district
court also did not err by failing to hold an evidentiary hearing because the court inquired into the particular circumstances and "the only material dispute was not about what happened but whether the district attorney's version of what he did was sufficient oversight." Id. Certainly Lyons points to no evidence he could have sought to introduce or discover at an evidentiary hearing which could have contradicted District Attorney Blodgett's version of events. Nor does he point even to a question he might have asked Blodgett. We therefore face similar facts as in Albertelli and so reach the same result--the wiretap was properly authorized.5

**c. Facial Sufficiency of the Wiretap Application**

Lyons also argues that the wiretap evidence should be suppressed because, even if the warrant was properly authorized, it did not make clear on its face that it had been reviewed by District Attorney Blodgett. This argument conflates two separate sections of the federal law governing wiretaps, Title 18, sections 2516 and 2518. Section 2516 sets out the substantive requirements for the authorization of a wiretap, including the requirement of review by the principal prosecuting attorney, while section 2518 sets out the procedure by which wiretaps can be requested. Nothing

---

5 Lyons also suggests that he had a right to confront District Attorney Blodgett. Again, he misunderstands the Confrontation Clause. See United States v. Mitchell-Hunter, 663 F.3d 45, 51-52 (1st Cir. 2011) (collecting "extensive case law declining to apply the confrontation right to various pre- and post-trial proceedings").
in section 2518 requires that a wiretap application itself contain proof that it has been reviewed by the principal prosecuting attorney. United States v. Vento, 533 F.2d 838, 859-60 (3d Cir. 1976) (Authorization letter did not need not be shown to the issuing judge.); see also United State v. Chavez, 416 U.S. 562, 575 (1974) (Evidence derived from a wiretap did not need to be suppressed where "misidentification of the officer authorizing the wiretap application [in the application] did not affect the fulfillment of any of the reviewing or approval functions required by Congress."). Instead, the application must only state "the applicant's authority to make such application." 18 U.S.C. § 2518(1).6

The designation letter made clear that District Attorney Blodgett authorized the application. Our conclusion that proof of review by the district attorney is not required on the face of the application also follows from United States v. Smith, 726 F.2d 852, 860 (1st Cir. 1984), in which we recognized that failure to include proof of authorization in the application could be remedied by subsequently produced evidence of authorization.

---

6 The distinction between the identity of the authorizing official, which must be present on the face of the application, and proof of authorization, which need not be included, is critical. Lyons mistakenly relies on United States v. Staffeldt, 451 F.3d 578, 584-85 (9th Cir. 2006), which holds that, in some cases, failure to provide the former on the face of the application is grounds for suppression. Here, however, the issue is the absence of the latter.
8. The Lyons Searches

In addition to the wiretaps, Lyons argues that the district court erred by denying his motion to suppress evidence obtained from the 2006 searches of his home, car, and person pursuant to warrants. First, Lyons argues that there was not probable cause for the search of his home. Second, he argues that the state justice's failure to sign the final page of each warrant means that the searches violated the Fourth Amendment of the United States Constitution. We reject both arguments and affirm the district court's denial of Lyons's motion to suppress.

a. Probable Cause For the Searches

Lyons challenges the warrants to search his home, car, and person using the same argument he first made about the wiretaps: that the subsequent decision by the district court that internet gambling is legal in Massachusetts means there was not probable cause to suspect him of a crime. He has again waived that argument by failing to raise it below and we therefore reject it without further discussion for the reasons stated above.

Lyons also brings a properly preserved challenge to the search of his home, arguing that there was no nexus between the evidence sought in the search warrant and his home. A valid warrant application must establish that there is probable cause to believe that the evidence described in it will be found in the place to be searched. United States v. Feliz, 182 F.3d 82, 86 (1st
Cir. 1999). The government need not show, however, that "the belief [is] . . . necessarily correct or more likely true than false." Id. at 87 (citing Spinelli v. United States, 393 U.S. 410, 419 (1969)). Instead, "[o]ur inquiry is whether the magistrate had a 'substantial basis' for concluding that probable cause existed." Id. at 86 (quoting United States v. Taylor, 985 F.2d 3, 5 (1st Cir. 1993)).

The trooper's affidavit submitted in support of the warrant application for Lyons's home contained sufficient evidence of a nexus between the evidence it sought and Lyons's home. The trooper stated under oath that "Lyons would go directly to his residence when he had completed his meets [with bettors.]" He also stated that "[b]ased on my training and experience and coupled with the intercepted conversations that I have reviewed regarding Todd Lyons, it is my opinion that Todd Lyons uses his residence as a place where he stores gaming records and money." We have previously held that the nexus requirement was met by weaker evidence. See, e.g., United States v. Ribeiro, 397 F.3d 43, 50 (1st Cir. 2005) (holding that direct trips between home and sites of drug deals and defendant's need to store large quantities of cash sufficient to demonstrate nexus); United States v. Barnes, 492

Lyons is correct that the affidavit does not describe these incidents with particularity, but provides no reason to believe the trooper's statement inaccurately describes what he and other troopers observed.
F.3d 33, 37 (1st Cir. 2007) (holding that "when a defendant sells drugs outside his home, it is reasonable to conclude that there is evidence of his drug dealing activity in the home"); Feliz, 182 F.3d at 88 (collecting cases). We therefore find that the warrant was supported by probable cause.

b. The Unsigned Warrants

Absent exceptions not present here, police may not search a person's home without a warrant. See, e.g., Kentucky v. King, 131 S. Ct. 1849, 1856 (2011). The Fourth Amendment to the United States Constitution provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The police seeking to search Lyons's home completed a written application to search it and swore in support of that application. The application recited facts establishing probable cause. The state judge reviewed the application, determined that probable cause existed, signed the application, and signed the accompanying affidavit. The warrant described particularly the place to be searched, and the persons or things to be seized.

---

8 Because the evidence Lyons seeks to suppress was, it appears from the record, found in his home, not his car or on his person, we discuss only the warrant for the search of his home. Our analysis would apply equally, however, to all three warrants.
The judge, however, unintentionally forgot to sign the warrant itself before the officers conducted the search. The following day, after the search was complete, state law enforcement officials noticed the omission. The prosecutor promptly returned that day to the same judge, who belatedly signed the warrant, at the same time writing a note explaining that his failure to sign previously "was inadvertent and of no substantive consequence."

Lyons speculates that the state judge in fact never saw or approved the warrant until he later signed it, but the evidence amply supports the district court's factual finding to the contrary. Cf. United States v. Dubose, 579 F.3d 117, 120 (1st Cir. 2009) (findings of fact on motions to suppress reviewed for clear error). Lyons alternatively claims that the record is defective (and an evidentiary hearing was therefore required) because it does not show "exactly" when, during the one-day interlude between issuance and signing, the Commonwealth noticed the error, or exactly how the judge was approached to correct the error. The simple answer to this assertion is that the "missing" facts are plainly immaterial to whether the warrant application was properly reviewed and whether the state court judge issued the warrant.

Lyons argues, finally, that the warrant was invalid precisely because it was not signed until after the search. This court has not previously ruled on whether a signature is required for a search warrant. But we see nothing in the Fourth Amendment
that conditions the validity of a warrant on its being signed. Similarly, while Federal Rule of Criminal Procedure 4(b)(1)(D) explicitly states that arrest warrants must be signed (as does Mass. R. Crim. P. 6(b)(1)), neither federal nor state rules of criminal procedure governing search warrants contain such a requirement. 9 See Fed. R. Crim. P. 41(e)(1); Mass. Gen. Laws ch. 276, § 1. Certainly that which the Fourth Amendment requires must appear on the warrant (a particular description of the "place to be searched" and "persons or things to be seized"). And a warrant does not issue unless it has been supported by an oath or affirmation and a neutral and detached magistrate makes a probable cause determination. See, e.g., King, 131 S. Ct. at 1864. But we see no convincing reason to find implicit in the Fourth Amendment a constitutional mandate that the magistrate who has made a probable cause determination also sign the warrant.

Our related precedent, while not directly on point, supports the conclusion that a signature is not required. In Burke v. Town of Walpole, 405 F.3d 66, 78 (1st Cir. 2005), we ruled that the police's inability to locate a signed copy of an arrest warrant

---

9 The Massachusetts Supreme Judicial Court has held that signatures are not required for a search warrant to be validly issued. Commonwealth v. Pellegrini, 405 Mass. 86, 90 (1989). Though compliance with state law is neither necessary nor sufficient for evidence's admission in federal court, see, e.g., United States v. Charles, 213 F.3d 10, 19 (1st Cir. 2000), we mention Massachusetts law here to underline that our conclusion is consistent with that of other courts.
did not preclude the state from proving with "imperfect[] evidence" that the warrant had in fact been issued. See also United States v. Pratt, 438 F.3d 1264, 1270 (11th Cir. 2006) (Where a search warrant is lost after the search it authorizes is conducted and therefore "is not in evidence at a suppression hearing," suppression is not necessary if "a prosecutor [can] prove, by a preponderance of the evidence, the missing search warrant's exact language describing the place to be searched and the persons or items to be seized."). If issuance of an arrest warrant can be established without a signed copy of the warrant, we see no reason why signing is necessary to prove issuance of a search warrant.

Our conclusion is strengthened by the consistent rejection of formalistic approaches to signatures in warrants by federal appellate courts in other contexts. Like other circuits, we have rejected the position that the copy of the warrant presented to a homeowner must bear a signature. See Sadlowski v. Benoit, 62 F. App'x 3, 5 (1st Cir. 2003) (unpublished) (per curiam); accord United States v. Beals, 698 F.3d 248, 264-65 (6th Cir. 2012) (holding that warrant was "not any less 'issued'" where judge signed only one copy and unsigned copy was presented to the defendant); United States v. Lipford, 203 F.3d 259, 270 (4th Cir. 2000) (failure to present signed copy of a search warrant to the person whose home is searched is "at most, a technical violation of
Federal Rule of Criminal Procedure 41(d), and not a violation of the Fourth Amendment.

The Second Circuit has gone further, noting that "the Fourth Amendment requires that . . . the judgmental function of drawing inferences from evidence and deciding whether probable cause exists be made by a neutral and detached magistrate," but that "nothing in the Fourth Amendment prevent[s a] magistrate from delegating" the "purely ministerial task" of signing the warrant to someone else. United States v. Turner, 558 F.2d 46, 50 (2d Cir. 1977) (approving a warrant application and issuance made entirely by telephone). The Eighth Circuit has held that Title III (the wiretap statute codified at 18 U.S.C. §§ 2510–2520), which is silent on whether wiretap orders must be signed, does not require a signature where "[t]he record reveals compliance with all the fundamental statutory safeguards that protect against unauthorized or unwarranted wiretap surveillance." United States v. Moore, 41 F.3d 370, 375 (8th Cir. 1994); see also United States v. Johnson, CRIM. 08-374, 2012 WL 2370434 (W.D. Pa. June 21, 2012) (same). But see United States v. Moore, 4:CR93-3035, 1993 WL 764485 (D. Neb. Dec. 28, 1993) (suppressing wiretap conducted under unsigned wiretap order where judge who failed to sign the order testified that he intended to sign it but could not recall what, if anything, he said to the requesting officers at the time). And in the context of arrest warrants, the Seventh Circuit has observed that
"[i]ssuing a warrant is not synonymous with signing a warrant" because while Federal Rule of Criminal Procedure 4(b)(1)(D) requires a judge's signature for arrest warrants issued pursuant to a criminal complaint, Rule 9 states that warrants for a defendant named in an indictment must still be issued by a judge but may be signed by a clerk of the court. United States v. Hondras, 296 F.3d 601, 603 (7th Cir. 2002); see also ISSUE, Black's Law Dictionary 908 (9th ed. 2009) (defining "issue" as "[t]o send out or distribute officially"). Certainly our own opinions and mandates are "issued" notwithstanding the absence of a signature.

Though none of these cases from other circuits address the precise question before us,10 taken together they show a consistent unwillingness to find a constitutional violation when

10 The majority of the few district court opinions on point reject the position that a warrant must be signed to be validly issued. See United States v. Jackson, 617 F. Supp. 2d 316, 320-21 (M.D. Pa. 2008) (holding that an unsigned warrant is valid if supported by sufficient "indicia of issuance"); United States v. Martin, 8:10-CR-305-T-33AEP, 2011 WL 722969, at *4 (M.D. Fla. Feb. 7, 2011) (holding that "the Court's sole inquiry should be to determine whether the search warrant was reviewed and issued by an appropriate judicial authority upon an examination of all relevant and credible evidence"); Perrin v. City of Elberton, GA, 3:03-CV-106(CDL), 2005 WL 1563530 (M.D. Ga. July 1, 2005) (holding that "in the absence of a judge's signature, a court may consider other evidence that the judge found probable cause and approved the warrant" but concluding there was insufficient evidence of such issuance); Johnson v. Kosciusko Police Dep't, 1:09CV169-M-S, 2010 WL 1237934 (N.D. Miss. Mar. 25, 2010) (holding the same in a section 1983 case). But see United States v. Evans, 469 F. Supp. 2d 893, 897-99 (D. Mont. 2007) (rejecting argument that a warrant could be said to have issued where judge "may well have" intended to sign it but failed to do so).
the express mandates of both constitution and rule have been satisfied. Given the clear and contemporaneous evidence that the state justice made a proper probable cause determination and approved the issuance of a warrant for execution, we decline to find in the lack of a signature a reason for suppression.

We do, though, add a note of caution: The presence of a signature provides easy and reliable proof that a warrant was in fact issued. An officer who observes that a warrant is unsigned might not be assured that it was actually issued, and might execute it at his peril if he has no other good reason to believe the warrant was issued. And when, as here, the warrant is not signed, proof of issuance becomes more involved and less certain. In many circumstances, the magistrate or judge may not recall reviewing or issuing the warrant by the time his belated signature is sought. For these reasons, we are confident that police will continue to have ample incentive to secure signatures. In any event, we find no sufficient reason to read a signature requirement into the Fourth Amendment, and we leave to any future revisers of Federal Rule of Criminal Procedure 41(e) whether to adopt such a presently-omitted requirement for search warrants.

9. Lyons's Money Laundering Conviction

Lyons challenges the sufficiency of the evidence for his conviction on two counts of money laundering under 18 U.S.C. § 1957, arguing that the statute applies only to the transmission
of profits from illegal activity, not to the transmission of gross receipts, and that the government failed to prove he transmitted profits. We have discussed Lyons's preservation of his sufficiency claims and the standard of review for such claims above. We repeat that we view Lyons's arguments as likely preserved by his general motion. Again, though, we need not formally resolve the preservation issue because, even reviewing the challenge de novo, interpreting the evidence in the light most favorable to the verdict, Lyons's argument fails.

Section 1957(a) provides (and provided in 2006 when the transmissions at issue here were made) that "[w]hoever . . . knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000" violates the law if the funds are "derived from specified unlawful activity." "Specified unlawful activity" is defined as a violation of any of the statutes or types of statutes listed in 18 U.S.C. § 1956(c)(7). "'Criminally derived property'" is "any property

11 Lyons's brief includes some discussion of the district court's instructions to the jury on this subject and his objection to them. The court's instructions, however, would be relevant only if Lyons were seeking a new trial rather than a reversal of the district court's denial of his Rule 29 motion and he has chosen not to do so. Lyons's statement of the issues, argument summary, and the portion of his brief dealing with this count all make clear that he has chosen to only challenge the sufficiency of the evidence. If this had simply been a case of unclear drafting, Lyons presumably would have explained in his reply brief that he intended to argue instructional error as well as sufficiency of the evidence. But he did not, even after the government, in its brief, pointed out the limited scope of his appeal.
constituting, or derived from, proceeds obtained from a criminal offense." 18 U.S.C. § 1957(f)(2). Until a definition of "proceeds" was added to section 1956 in 2009, the term was undefined. See Fraud Enforcement and Recovery Act of 2009, Pub L. No. 111-21 § 2, 123 Stat. 1617. The 2009 amendment was a response to United States v. Santos, 553 U.S. 507 (2008), which interpreted the word "proceeds" in a closely related statute, 18 U.S.C. § 1956, to refer only to the profits from illegal activity, rather than gross receipts. The government does not dispute that the word "proceeds" meant "profits" in section 1957 as well as section 1956 prior to 2009.

Santos further explained, however, that to prove a defendant transmitted "profits . . . the prosecution needs to show only that a single instance of specified unlawful activity was profitable and gave rise to the money involved in a charged transaction." Id. at 520. If the underlying crime can be accomplished through a single transaction then the prosecution need not show that the profits from that particular act were not offset by losses elsewhere in the criminal conspiracy, but must instead only show that the particular transaction charged consisted of at least $10,000 in profits. Id. Lyons does not dispute that 18 U.S.C. § 1957, which criminalizes "a monetary transaction" that meets certain criteria, can be violated by a single act. There was therefore no need for the government to prove that SOS as a whole
was profitable in order to convict Lyons under that statute. All the government needed to prove was that the proceeds of the particular transactions charged in the indictment were "profits" of "specified unlawful activity." Santos, 553 U.S. at 520 n.7.

There was sufficient evidence for such a finding. Lyons was acquitted of money laundering on all but two counts, each of which was based on transfers from Lyons's customer Thomas Belekewicz. The indictment describes the underlying crime simply as "unlawful gambling activity" without specifying a particular statute (besides section 1957) that the transfers violated. However, the previous section of the indictment, charging money laundering under section 1956, specifies that the underlying crime of "illegal gambling activity" was a violation of 18 U.S.C. § 1955 (the same statute at issue in Santos), which criminalizes operation of an illegal gambling business, and 18 U.S.C. § 1084, the Wire Act. Violations of both statutes are "specified unlawful activity" as that term is defined under 18 U.S.C. § 1957(f)(3) because they are offenses listed in 18 U.S.C. § 1961(1), and therefore fit the definition of unlawful gambling activity by 18 U.S.C. § 1956(c)(7)(A).

Belekewicz testified that he and his business partner Ed Doherty placed bets on sporting events using the telephone or internet. By receiving such bets, SOS violated the Wire Act. 18 U.S.C. § 1084(a). On November 17, 2005, following Lyons's
instructions, Belekewicz attempted to transfer $20,381 to Benevolence Funding, a company controlled by Robert Eremian. This transfer constituted SOS's profits from its violation of the Wire Act by receiving bets from Belekewicz and Dohertry because the transfer represented the difference between Belekewicz's winnings and losses over those bets. Similarly, an $86,656 transfer (also made per Lyons's instructions) was "the accumulation of a few weeks" of Belekewicz's losses and so constituted SOS profits. There was therefore sufficient evidence for a reasonable jury to convict Lyons on each money laundering count because the evidence was sufficient to show that, on both occasions, Lyons caused the transmission or attempted transmission of at least $10,000 in profits from unlawful activity. The fact that Lyons or SOS may have lost money on other bets does not insulate Lyons from liability for these charged bets.

10. Lyons's Travel Act Convictions

Lyons challenges the sufficiency of the evidence for his conviction on four counts of violating the Travel Act, 18 U.S.C. § 1952, on the same grounds upon which he challenged his money laundering convictions. Lyons was convicted of four counts of "travel[ling] in interstate or foreign commerce or us[ing] the mail or any facility in interstate or foreign commerce, with intent to . . . distribute the proceeds of . . . any business enterprise involving gambling." 18 U.S.C. § 1952(a), (b). The indictment
charged four specific instances in 2005 in which Lyons sent money to Antigua via FedEx. Lyons argues that there was no evidence these transactions constituted profits. It is undisputed, though, that SOS agents collected losses from bettors, paid out winnings, deducted their commission, and only then remitted the remainder to SOS. Lyons functioned as a bank for SOS in Massachusetts, collecting these profits from SOS agents and paying out extra money to agents who needed it to cover large winnings. A reasonable jury could easily have concluded, therefore, that the money he sent to SOS in Antigua constituted proceeds of the SOS operation in Massachusetts even if we assume that the term "proceeds" under the Travel Act means "profits."

11. Lyons's UIGEA Convictions

Lyons also challenges his convictions on ten counts of violating the Unlawful Internet Gambling Enforcement Act, 31 U.S.C. §§ 5361-67. Lyons argues that it was impossible to violate the statute until certain regulations implementing it were passed. See Prohibition on Funding of Unlawful Internet Gambling, 73 F.R. 69382-01 (Nov. 18, 2008). These regulations clarify liability for financial institutions under the law. See 31 C.F.R. § 132.2. As applied to this case not involving a charge against a financial institution, UIGEA was adequately clear before these regulations were passed. The statute prohibits the knowing acceptance of certain financial instruments "in connection with the participation
of another person in unlawful Internet gambling." 31 U.S.C. § 5363. "Unlawful Internet gambling," in turn, is defined as "to place, receive, or otherwise knowingly transmit a bet or wager by any means which involves . . . the Internet where such bet or wager is unlawful under any applicable Federal or State law . . . ." 31 U.S.C. § 5362(10)(A). It is, as we have already noted, illegal to transmit or receive a sports bet in interstate commerce under the Wire Act even if placing the bet is legal at both ends of the transmission. 18 U.S.C. § 1084(a). The Wire Act is a federal law, and therefore transmitting or receiving bets is "unlawful gambling" as that term is defined in UIGEA. The final implementing regulations for UIGEA do not alter this analysis. It was therefore possible to violate the statute before the implementing regulations were passed. Nor was the statute so vague on its face that its enforcement was unconstitutional. See Interactive Media Entm't & Gaming Ass'n Inc. v. Atty. Gen. of U.S., 580 F.3d 113, 115-117 (3d Cir. 2009) (explaining in more detail why UIGEA survives such a facial challenge). We therefore affirm Lyons's UIGEA convictions.

12. The Prosecutor's Purported Reference to Lyons's Silence

Lyons presses his argument, first made at trial, that the prosecutor improperly referred before the jury to Lyons's decision not to testify, violating his Fifth Amendment right against self-incrimination. The government agrees that our review of this objection is de novo. The applicable test we apply is well
established. See United States v. Rodriguez-Velez, 597 F.3d 32, 44 (1st Cir. 2010). "A comment on the defendant's failure to testify . . . infringes the defendant's Fifth Amendment rights whenever 'the language used [by the prosecutor is] manifestly intended or [is] of such character that the jury would naturally and necessarily take it to be a comment on the failure of the accused to testify." Id. (quoting United States v. Glantz, 810 F.2d 316, 322 (1st Cir. 1987)).

Lyons's counsel argued at trial that Lyons "didn't think that he was doing anything wrong," supporting this argument with various examples of actions he said Lyons would not have taken if he had believed he was acting illegally. In closing, the prosecutor responded as follows:

Now there's been a lot of talk about, what did the defendants know? What did they intend? What did they believe? And [Lyons's counsel] wants to get up here and tell you what Todd Lyons thought. Now, I want you to check your notes, check the record, and see if there is any evidence before you about what Todd Lyons thought, or if there's any evidence from any witness about conversations between them and Todd Lyons where Todd Lyons expressed his opinion about the legality of Sports Off Shore. I suggest to you there is no evidence at all.

The prosecutor went on to suggest that the jury should infer Lyons's mental state from his actions. After the closing argument, Lyons's counsel objected to this statement and the district court offered to give a curative instruction. Lyons's counsel indicated that he did not want to "highlight it right now" but did request
and received an instruction on the Fifth Amendment when other jury instructions were given.

We have made clear that "[w]here the defendant has presented a defense . . . the government is permitted to discuss competing inferences from the evidence on the record." United States v. Glover, 558 F.3d 71, 77 (1st Cir. 2009). Similarly, the prosecution may comment on the lack of evidence for a defense theory. United States v. Wilkerson, 411 F.3d 1, 8 (1st Cir. 2005) (prosecutor did not violate the Fifth Amendment "when he said 'there's no real evidence' that [defendant] did not go up the alley and 'pretty much nothing' to say that [he] ran up the driveway"). The government commented on the lack of evidence to support a defense theory, not on Lyons's failure to testify. And the possibility that jurors may have inferred, from the comment actually made, a comment not actually made arises from the very nature of the defense raised, not from any uninvited effort by the government to carry its burden. We affirm the district court's ruling on this issue as well.

13. Venue in Massachusetts for Eremian

Shortly before trial, Eremian's counsel requested an instruction on venue. When the district court made clear it could not rule on the request without further briefing, he promised to provide it by the end of the day, adding that "[i]f I don't file it by 5:00 . . . today, it means I'm not requesting it." He did not
file any further briefing and therefore knowingly waived the issue, precluding any appellate review. See Fed. R. Crim. Pro. 12(e); United States v. Walker, 665 F.3d 212, 228 (1st Cir. 2011) ("[A] party's failure to raise Rule 12(b)(3) defenses prior to trial," including venue, "constitutes a waiver in the classic sense and, thus, precludes appellate review of the defaulted challenge.").

14. Eremian's RICO Conspiracy Conviction

Eremian was convicted on one count of racketeering conspiracy and one count of racketeering, only the latter of which he challenges. The prosecution may prove racketeering through, among other things, proof of collection of an unlawful debt. 18 U.S.C. § 1962(c). The indictment listed by name four people from whom Eremian purportedly collected an unlawful debt. Each testified at trial that he lived in Florida and paid money to Eremian to settle gambling debts.

A debt is "unlawful" under § 1962(c) if it is "(A) incurred or contracted in gambling activity which was in violation of the law of the United States, a State or political subdivision thereof, . . . and (B) . . . was incurred in connection with the business of gambling in violation of the law of the United States." 18 U.S.C. § 1961(6). We have already noted that the bets placed by SOS bettors were illegal under both federal and Florida law and such bets were incurred "in connection with the business of gambling." There was therefore more than sufficient evidence to
convict Eremian of collecting an illegal debt and, hence, of racketeering.

15. Adequacy of the Indictment

Eremian also argues that instructing the jury on Florida law to help it determine whether the debts he collected were unlawful constituted a constructive amendment of the indictment because the indictment did not specifically mention Florida law. The indictment was clear that Eremian lived in Florida and conducted his business for SOS there and that he was accused of collecting an unlawful debt from specific people who testified that they interacted with him in Florida. The indictment cited 18 U.S.C. § 1961(6), which defines an unlawful debt as "a debt . . . incurred or contracted in gambling activity which was in violation of the law of the United States, a State or political subdivision thereof." The indictment also described these debts as those "incurred in connection with the business of gambling in violation of the laws of the United States and the law of the Commonwealth of Massachusetts."

Though Florida, unlike Massachusetts, was not explicitly mentioned in the indictment, Eremian knew he was being charged with collecting a debt, unlawful under state or federal law, while residing in Florida. He was therefore on notice that Florida law would likely be at issue. See United States v. Vega Molina, 407 F.3d 511, 525 (1st Cir. 2005) ("[E]rroneous statutory citations in
an indictment do not constitute grounds for reversing a conviction, as long as the defendant was on fair notice of the charges against him."); United States v. Celestin, 612 F.3d 14, 24-25 (1st Cir. 2010) (no constructive amendment where defendant had "notice of the various theories of liability on which he could be convicted"); United States v. Hernández, 490 F.3d 81, 84 (1st Cir. 2007) (same).

16. Sentencing and Forfeiture

Lyons was sentenced to 48 months in prison while Eremian was sentenced to 36 months. Lyons and Eremian do not dispute that their sentences were within the range proscribed by the United States Sentencing Guidelines or that the guideline ranges for their convictions were properly calculated. Lyons and Eremian are less clear on what they are challenging, but they reference both the Eighth Amendment and the reasonableness of their sentences under the guidelines and so we will treat them as appealing their sentences on both bases.

A sentence violates the Eighth Amendment's prohibition of "cruel and unusual punishment if it is 'grossly disproportionate to the underlying offense.'" United States v. Raymond, 697 F.3d 32, 40 (1st Cir. 2012) (quoting United States v. Polk, 546 F.3d 74, 76 (1st Cir. 2008)). If, after comparing the "'gravity of the offense and the harshness of the penalty!'" we conclude there is no "gross disproportionality . . . the inquiry ends there." Raymond, 697 F.3d at 40 (quoting Solem, 463 U.S. at 290-91). That is the case
here—Lyons and Eremian were key players in multi-million-dollar gambling operation that lasted for more than a decade. Like "most efforts to demonstrate gross disproportionality[, this one] fail[s]." United States v. Polk, 546 F.3d 74, 77 (1st Cir. 2008). Lyons's and Eremian's challenges to the reasonableness of their sentences under the guidelines fail as well. We review the reasonableness of sentences for abuse of discretion. United States v. Tavares, 705 F.3d 4, 24 (1st Cir. 2013). "[A] defendant who protests his within-the-range sentence on this ground must adduce fairly powerful mitigating reasons and persuade us that the district court was unreasonable in balancing pros and cons." United States v. Medina-Villegas, 700 F.3d 580, 584 (1st Cir. 2012) (internal quotation marks omitted). Lyons and Eremian have even more trouble meeting this burden because their sentence was "within a properly calculated [guideline sentencing range.]" Id. Lyons's and Eremian's sentences were procedurally reasonable because the district court understood the guidelines to be discretionary and properly considered the relevant factors under 18 U.S.C. 3553(a). Lyons and Eremian nonetheless argue that their sentences are substantively unreasonable for two main reasons.

First they argue their sentences are unreasonable because they exceed those of other SOS conspirators who were not charged or did not spend time in jail. The district court found that Lyons's and Eremian's roles were more central to SOS than those of others.
who were not charged (except, presumably, for Richard Sullivan and Robert Eremian who are fugitives). Moreover, many of the other SOS agents cooperated with the government's investigation and therefore are not directly comparable to Lyons and Eremian for sentencing purposes. United States v. Mateo-Espejo, 426 F.3d 508, 514 (1st Cir. 2005) ("[I]t would seem patently unreasonable to endorse a regime in which a defendant could steadfastly withhold cooperation from the authorities and then cry foul when a coconspirator benefits from rendering substantial assistance to the government.").

Second, Lyons and Eremian argue that their sentences are unreasonable because they exceed the maximum sentences for their Wire Act convictions and the guideline range for federal statutes specifically criminalizing the operation of a gambling business. The government agrees that "RICO and RICO conspiracy convictions largely drove the offense level calculation." But there is nothing unreasonable about sentencing Lyons and Eremian for violating RICO when they were actually convicted of violating RICO. A court could perhaps have considered Lyons and Eremian's argument in making a downward departure, but the district court certainly did not abuse its discretion by declining to do so, nor do Lyons and Eremian cite any precedent to the contrary. Because "[w]e generally respect the district court's sentence as long as the court has provided a plausible explanation, and the overall result is defensible," we do
so in this case as well. United States v. Innarelli, 524 F.3d 286, 292 (1st Cir. 2008).

Lyons's and Eremian's remaining arguments are even less deserving of substantial discussion. The rule of lenity is a rule of statutory interpretation and does not, contrary to Lyons's and Eremian's assertions, apply to the reasonableness of sentences. United States v. Aponte-Guzman, 696 F.3d 157, 160 (1st Cir. 2012). Nor was the court obligated to depart downward based on Lyons's and Eremian's argument (which the jury also apparently rejected) that they had a good-faith belief their conduct was legal. Finally, Lyons's and Eremian's family ties were considered by the district court in determining their sentences and its decision not to depart downward on that basis was not an abuse of discretion.

Finally, we affirm the forfeitures as well. The district court, after a three-day bench trial, determined the total amount of criminal proceeds\(^\text{12}\) garnered by SOS and reasonably foreseeable by Lyons ($24,504,126) and Eremian, ($7,766,095), and then entered forfeiture judgments against them in those amounts. See United States v. Hurley, 63 F.3d 1, 22-23 (1st Cir. 1995) (holding that forfeiture judgments against one participant in a conspiracy equal to the reasonably foreseeable criminal proceeds obtained by others in the conspiracy are appropriate). The district court explained

\(^{12}\) Lyons and Eremian have not challenged the method the district court used to calculate their forfeiture judgment, only the proportionality of the total figure.
how it arrived at the total forfeiture amount in a detailed, thoughtful, and well-researched opinion. Lyons and Eremian do not challenge its factual conclusions in any detail, though they dismiss its factual finding in a conclusory manner in their reply brief. We review factual findings in sentencing for clear error, see United States v. Cintron-Echautegui, 604 F.3d 1, 5 (1st Cir. 2010), a standard Lyons and Eremian have not even come close to beginning to meet.

Lyons and Eremian contend that the imposition of the large forfeiture judgments against them was disproportionate given the lack of similar judgments against other participants in the SOS conspiracy. We have held, however, that it is entirely appropriate to impose "an order substituting other property of each defendant up to the value of the criminal proceeds for which the defendant was jointly and severally liable." United States v. Candelaria-Silva, 166 F.3d 19, 44 (1st Cir. 1999). The forfeiture judgments against Lyons and Eremian are also proportionate for the same reasons as their prison sentences are proportionate—they played a larger role in SOS than others and did not cooperate with prosecutors.

III. Conclusion

For the reasons stated above we affirm Lyons's and Eremian's convictions and sentences.

So ordered.
UNITED STATES COURTS OF APPEALS
FOR THE SIXTH CIRCUIT

DICE CORPORATION

Plaintiff-Appellant,

v.

BOLD TECHNOLOGIES, INC.

Defendant-Appellee.

ON APPEAL FROM THE
UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN

BEFORE: GUY, GIBBONS, and ROGERS, Circuit Judges.

JULIA SMITH GIBBONS, Circuit Judge. Plaintiff-appellant Dice Corporation and defendant-appellee Bold Technologies are competitors that provide services and license software to companies in the alarm industry. Dice claims that Bold committed a host of intellectual property violations when converting one of Dice’s former customers to its systems. The district court granted Bold’s motion for summary judgment on all of Dice’s claims and denied Dice’s motions for reconsideration and indicative ruling. For the following reasons, we affirm.

I.

A.

Dice Corporation and Bold Technologies are in the same business—both license software to companies in the alarm industry. Alarm companies monitor signals sent from their respective subscribers’ alarm systems. When an alarm signal is tripped, the alarm company contacts the appropriate authorities such as the police or fire department. Alarm companies collect an impressive amount of data. The data typically consists of names, addresses, contact information,
billing information, and information regarding the type and location of alarms. As a general matter, both companies’ software monitors alarm signals and compiles information in databases. Dice’s software is known as Dice software; Bold’s is licensed under the trade name Manitou.

Despite providing similar services, the technical features of their software are significantly different. By way of quick background, computers operate in a binary number system: 0 for off and 1 for on. Current computers are capable only of executing functions based on this basic language consisting of strings of 1’s and 0’s. This is known as object code. Computer programming languages—such as C++ and Thoroughbred Basic—facilitate human programming by obviating the need for programmers to write in cumbersome object code. The text of these languages is known as source code. Whether directly or indirectly, the instructions written in source code are ultimately translated into object code so that commands can be executed by the computer. See generally Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 305 (S.D.N.Y. 2000). Dice software is written using the programming language Thoroughbred Basic and runs on the Linux operating system. Manitou is written in the C++ and Visual Basic languages and runs on the Windows operating system.

B.

This dispute stems from a customer defection. ESC Central was a Dice customer for a decade. In 2011, it transitioned to Bold. Switching software systems is no easy task. The conversion process must be undertaken carefully because the alarm company continues to monitor alarm signals from its subscribers. The transition must be seamless to ensure that the new software is interpreting the incoming alarm signal in the same manner as the old so that no alarm signals are misread or missed. As Bold’s chief of operations explained:

After the customer data is extracted and converted, there will be a period of time, usually about 3 months when the customer’s central station is running live on the
old software, but the new software is running in parallel on different servers. The purpose of running the two software systems in parallel is to ensure that the new software is monitoring the alarm signals consistent with the old software. After this period is completed the customer will go live on the new software and will often terminate its license for the old software.

Following this protocol, Bold first extracted ESC Central customer data from Dice’s software databases. This data—names, addresses, etc.—is owned by ESC Central and not by Dice. Matt Narowski, a current Bold employee and former Dice employee, wrote the computer program (“Extraction Program”) used to extract customer data from Dice’s database. He explained that he wrote the program using information available to the public together with general knowledge of computer programming; he did not read, review, copy, or rely upon any information about Dice source or object code; the Extraction Program does not contain any Dice source or object code; and, since being employed at Bold, he has not seen a copy of Dice source or object code. And he explained that “the database files where the customer data is stored are not subject to any Dice security features and can be accessed by anyone who has a copy of Thoroughbred Basic, which Bold licensed from that company.”

Not so, says Dice. Dice maintains that Bold used and copied Dice’s proprietary software in operating the Extraction Program. Clifford Dice stated that he “analyzed the conversion program created by” Narowski and concluded that “[t]he program which Bold has created for converting information belonging to Dice customers cannot operate without access to Dice software and the source code contained within that software.”

C.

Following extraction, the Bold and Dice software systems were run in parallel from June 2011 to August 2011. Although not aware at the time that ESC Central was converting to Bold’s Manitou, Dice subsequently became aware through Facebook activity by ESC Central’s vice
president, Kristi Harris Jennings. Immediately thereafter, Dice’s Director of Software Development, Julie Coppens, logged into the ESC Central system. She found that someone had accessed Dice’s ALSCHART file. Coppens testified that although ESC Central had disconnected Dice, it had not removed access to a phone connection. ESC Central described this as “illegal entering,” and sent a cease and desist letter, threatening suit if Dice did it again. Dice, on numerous occasions, admitted that it has no evidence that it was anyone at Bold who accessed the file.

The ALSCHART is a file containing a master list or database of alarm codes. Manufacturers code\(^1\) outgoing alarm signals to identify the type of emergency. For example, a fire signal may be coded “F” by one company and “1” by another. The alarm panel sends these signals to receivers at alarm companies where the information is converted into Dice’s standard and compiled in the ALSCHART, a part of Dice’s software. Dice’s receiver-drivers software performs the conversion from manufacturers’ signals to Dice’s standard. Dice contends that the ALSCHART and its receiver drivers are proprietary. According to Dice, its standards are unique.

D.


\(^{1}\)These are not computer codes in the same way that object and source code are computer code—\textit{i.e.}, they do not function to allow humans to operate the computer. Alarm codes function as labels indicating the type of alarm.
Nos. 12-2513, 13-1712

*Dice v. Bold*

Program impermissibly accessed and utilized Dice’s proprietary code; (2) former Dice employee and current Bold employee Amy Condon accessed Dice servers and initiated file transfers of proprietary software; and (3) Bold circumvented Dice security protections to access protected material.

Clifford Dice was deposed on February 29, 2012. Bold did not provide Dice with a copy of the Extraction Program until May 14, 2012. Bold moved for summary judgment on June 29, 2012, attaching twenty exhibits covering most of the factual material discussed thus far. Dice filed a cursory response. The response relied in large part on an attached affidavit in which Clifford Dice attested that he had “analyzed the conversion program created by former Dice and current Bold employee Matt Narowski.” He claimed that the Extraction Program could not “operate without access to Dice software and the source code contained within that software.”

Bold’s reply attached a rebuttal expert report from Dr. William McUmber. The report analyzed the Extraction Program and concluded that:

Bold Extract only performs the task of pulling data from the customer’s database so that it can be transferred to a different system. . . . Bold Extract does not and cannot read program source code, and does not need to use the Dice source code to perform the data extraction. Bold Extract has no decryption functions, either for data or source code. All of the customer data Bold Extract pulls from the database is unencoded and requires no special handling with decoding functions. No proprietary knowledge is required to write Bold Extract. All of the information that would be needed to write it can be found in ThoroughBred reference guides.

Dice requested that Bold produce Dr. McUmber for deposition prior to filing its summary judgment motion. On this basis, Dice moved to strike Dr. McUmber’s report. Dr. McUmber was deposed on September 26, 2012. Dice did not move to file a sur-reply or supplement the record following the deposition. Dice’s motion to strike was eventually denied as moot.
The district court rejected Dice’s claims in a forty-page opinion, finding them conclusory and devoid of factual support. Dice moved for reconsideration on two grounds. First, Dice claimed that the district court improperly credited the affidavit of Narowski, which Dice claimed was at odds with his deposition testimony. Second, Dice claimed that new evidence—a copy of the “entire extraction program”—was improperly withheld until after Bold filed its motion for summary judgment. Dice claimed that at the time of Dr. McUmber’s deposition, Bold produced for the first time the File List used by Bold’s Extraction Program (known as “FILELIST.txt”). “Receipt of the entire program,” Dice claimed, “permitted [Dice] for the first time to quantify the extent to which [Bold’s program was dependent upon Dice source code] and “also permitted [Dice] to disprove the [notion] that [Bold’s] extraction program simply utilized commercially-available software produced by Thoroughbred.”

Dice attached a comparison highlighting several areas which, Dice claimed, showed literal copying. But as the district court noted in its opinion denying the motion for reconsideration, Clifford Dice did not explain how this evidence demonstrated that Bold used Dice’s source code. “Instead he attache[d] a computer printout to his affidavit that [Bold] charitably describes as ‘virtually incomprehensible.’ . . . The Court’s own review, in contrast, finds the document completely incomprehensible.” The printout contained hundreds of pages of unexplained computer code. Moreover, the File List on which Clifford Dice’s analysis was based was not attached to Dice’s motion. Dice claims that the failure to attach this document was inadvertent.

After filing its motion for reconsideration but before the district court ruled on that motion, Dice filed a notice of appeal. Subsequently, the district court denied Dice’s motion for reconsideration. Dice did not amend its notice of appeal within 30 days of that date. On May
16, 2013, Dice filed a motion for indicative ruling and relief from judgment pursuant to Federal Rules of Civil Procedure 60(b) and 62.1. Dice asserted that its clerical error in attaching the wrong exhibit caused the district court to deny the motion for reconsideration and asked the district court to enter an order indicating that it would grant Dice’s motion for reconsideration if the court of appeals remanded for that purpose. The district court denied the motion, holding that Dice again failed to explain how the proffered evidence demonstrated that Bold misappropriated its property.

Dice filed an amended notice of appeal within 30 days of the denial of its motion for indicative ruling expressly seeking review of the order granting Bold’s motion for summary judgment and the order denying Dice’s motion for indicative ruling; it did not seek review of the reconsideration order.

II.

The first question is one of jurisdiction. Dice attempts to appeal the district court’s denial of its motion for indicative ruling. Under Rule 62.1, a district court may make certain indicative rulings on motions that the court lacks authority to grant because of a pending appeal. A district court may defer considering the motion, deny the motion, or state that it would grant the motion or that the motion raises a substantial issue. See Fed. R. Civ. P. 62.1(a).

Corresponding to Rule 62.1 is Federal Rule of Appellate Procedure 12.1. Rule 12.1(b) provides that “if the district court states that it would grant the motion or that the motion raises a substantial issue, the court of appeals may remand for further proceedings.” Bold argues that because Rule 12.1(b) does not expressly provide for circumstances in which the district court denies a motion for indicative ruling, courts of appeal lack jurisdiction to entertain appeals from such motions. We are unaware of any case which so holds. See Fed. R. App. P. 12.1 advisory
committee’s notes (citing Jordan v. Bowen, 808 F.2d 733, 736–37 (10th Cir. 1987) (refusing to review order denying motion for indicative ruling where party failed to appeal from that order)); see also Ray v. Pinnacle Health Hosps., Inc., 416 F. App’x 157, 161 (3d Cir. 2010) (reviewing denial of motion for indicative ruling). Nor do we believe Rule 12.1 requires a party to wait until its initial appeal is adjudicated, file a new Rule 60(b) motion, and then appeal that motion’s denial. Rule 12.1 does not foreclose our review.

Next is Dice’s unappealed motion for reconsideration. In its amended notice of appeal, Dice did not mention the order denying its motion for reconsideration. Bold argues that under Federal Rule of Appellate Procedure 4(a)(4)(B)(ii) and this court’s opinions construing that rule, we lack jurisdiction to review the order denying reconsideration as well as the evidence put forward in Dice’s motion.


We consider all arguments asserted prior to the final disposition of a case if the party indicates in its notice of appeal that it appeals either the final judgment or the final order. Id. at 906. Where the notice of appeal limits the orders appealed, we will not, “absent specific mention
in the notice of appeal, entertain issues raised in post-judgment motions.” *Id.* However, “[t]o the extent that the post-judgment motions relate to issues raised before judgment, the appellate court will deal with them anyway.” *Id.* Although the case law speaks of issues raised before the “final order” or the “final judgment,” there is no principled reason to hold that this language bars consideration of issues raised before the last order appealed. The only concern motivating this jurisprudence is compliance with the Federal Rules of Appellate Procedure’s notice requirement. *See id.* Parties receive the same notice of the issues on appeal whether they were raised in a notice of appeal of a motion granting summary judgment or subsequent motion for indicative ruling. What matters is that the issues flagged in the notice of appeal have already been raised. The dividing line is the last appealed judgment: issues raised before the last appealed judgment will be considered, issues raised after will not. Here, the last appealed judgment was the motion for indicative ruling.

Dice raised two issues in its motion for reconsideration. The first issue was whether the district court erred in relying on Narowski’s affidavit. This issue was before the district court in Bold’s motion for summary judgment. The second issue was whether Bold’s untimely production of the File List prevented Dice from demonstrating that Bold misappropriated its copyrighted source code. Dice’s motion for indicative ruling argued that the district court erred in denying the motion for reconsideration because Dice inadvertently attached the wrong exhibit. The motion for indicative ruling, relying on the same arguments and evidence and the properly attached exhibit, sought to cure that defect. Indeed, it would be impossible to consider the motion for indicative ruling—which was properly appealed—without considering the motion for reconsideration. Accordingly, this court has jurisdiction to consider the issues and facts raised in Dice’s motion for reconsideration.
III.

It is the parties, in our adversarial system, who frame the issues before the court. This is true of both factual and legal arguments. The rules of civil procedure and standards of appellate review acknowledge this. The nub of this dispute is the district court’s summary judgment order. Rule 56(c) requires a party objecting to a motion for summary judgment to support its assertions by “citing to particular parts of materials in the record.” Accordingly, we do not “entertain on appeal factual recitations not presented to the district court” when reviewing a district court’s decision.” Chi. Title Ins. Corp. v. Magnuson, 487 F.3d 985, 995 (6th Cir. 2007) (quoting Guarino v. Brookfield Twp. Trustees, 980 F.2d 399, 404 (6th Cir. 1992)). The “proper focus is on the factual evidence submitted below.” Id. at 996; Cacevic v. City of Hazel Park, 226 F.3d 483, 491 (6th Cir. 2000) (“Although [plaintiffs] proffered evidence that might or might not show a genuine issue of material fact after the district court had granted the defendants’ motion for summary judgment, that evidence will not be considered by us on review.”); Estate of Mills v. Trizec Props., 965 F.2d 113, 115 (6th Cir. 1992). “This burden to respond is really an opportunity to assist the court in understanding the facts. But if the non-moving party fails to discharge that burden . . . its opportunity is waived and its case wagered.” Guarino, 980 F.2d at 405.

The same is true of legal arguments. This court requires “timely and reasoned presentation of non-jurisdictional issues to avoid forfeiture.” Winnett v. Caterpillar, Inc., 553 F.3d 1000, 1006 (6th Cir. 2009). “It is well-settled that this court’s ‘function is to review the case presented to the district court, rather than a better case fashioned after an unfavorable order.’” Armstrong v. City of Melvindale, 432 F.3d 695, 700 (6th Cir. 2006) (internal alterations and quotation marks omitted) (quoting Barner v. Pilkington N. Am., Inc., 399 F.3d 745, 749 (6th
Nos. 12-2513, 13-1712

Dice v. Bold

Cir. 2005). Arguments not squarely presented to the district court are not reviewed on appeal. See, e.g., Thurman v. Yellow Freight Sys., Inc., 90 F.3d 1160, 1172 (6th Cir. 1996).

With these parameters in mind, we review the district court’s order granting summary judgment de novo, see Crouch v. Honeywell Int’l Inc., 720 F.3d 333, 338 (6th Cir. 2013), and, treating a denial of indicative relief as we would a Rule 60(b) motion, we review the district court’s order denying Dice’s motion for indicative ruling for abuse of discretion, see Ray, 416 F. App’x at 161 n.3. As will be discussed in greater detail below, Dice’s appeal suffers from both aforementioned ailments—it presents new legal arguments supported by previously unmentioned record evidence.

IV.

A.

Dice argues that the district court erred in granting summary judgment to Bold on the MUTSA claim. A claim for misappropriation of trade secrets, as the cause of action suggests, requires: (1) a trade secret; and (2) misappropriation. See Mich. Comp. Laws § 445.1902.2

A trade secret consists of two component parts. It is information that derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who could obtain economic value from its disclosure or use. Id. § 445.1902(d). And the information must be the subject of reasonable efforts under the circumstances to maintain its secrecy. Id. As a general matter, trade secret law does not protect “an idea which is well known or easily ascertainable.” Manos v. Melton, 100 N.W.2d 235, 238 (Mich. 1960). “Trivial advances or differences in formulas or process operation are not

2 The district court and the parties rely on Stromback v. New Line Cinema’s articulation of a three-part trade secret claim. 384 F.3d 283, 302 (6th Cir. 2004). Stromback explicitly stated that the three-element trade-secret claim was the common-law claim and that the common-law claim was displaced by MUTSA. Id.
protectable as trade secrets.” *Id.* at 239 (internal quotation marks omitted); *Agency Solutions.Com, LLC v. Trizetto Grp., Inc.*, 819 F. Supp. 2d 1001, 1017 (E.D. Cal. 2011) (“Proprietary ways of doing the same thing that others in the same field do are not trade secrets.”). “Of critical importance here, to be worthy of trade secret status, the secret information must afford the owner a competitive advantage by having value to the owner and potential competitors.” *Daimler-Chrysler Servs. N. Am., LLC v. Summit Nat’l, Inc.*, 289 F. App’x 916, 922 (6th Cir. 2008) (applying MUTSA).

MUTSA defines misappropriation as acquisition, disclosure, or use of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means. *See* Mich. Comp. Laws § 445.1902(b).

Dice argues that Bold misappropriated two trade secrets: (1) the ALSCHART; and (2) its receiver drivers software.

**1.**

Dice argues that the district court erred in concluding that the data obtained from the ALSCHART file via the Thoroughbred query was not a trade secret. Again, the ALSCHART is a file containing a master list or database of alarm codes. Dice argues that because the ALSHCART contains codes converted to Dice’s standards, the ALSCHART was subject to trade secret protection.

Dice fails to explain how this information, even if uniquely coded, is a trade secret. The ALSCHART is a compilation of labelling codes created by manufacturers, not Dice. The codes were collected by Dice’s customers, not Dice. Dice has not put forward an explanation of how the value of its unique labelling is derived from it not being readily ascertainable by proper means. And Dice has not produced any evidence to that effect. *See* Mich. Comp. Laws §
Nos. 12-2513, 13-1712

*Dice v. Bold*

450.1902(d); *see also* Daimler-Chrysler, 289 F. App’x at 922 (plaintiff bears the burden to produce sufficient evidence to suggest that information derives independent economic value secrecy); Utilase, Inc. v. Williamson, 188 F.3d 510, 1999 WL 717969, at *6 (6th Cir. Sept. 10, 1999) (plaintiff must identify trade secret with specificity); Dura Global Techs., Inc. v. Magna Donnelly Corp., 662 F. Supp. 2d 855, 859 (E.D. Mich. 2009) (same).

In addition, Dice failed to present competent evidence of misappropriation to the district court. Noting the fact that Dice did not cite any record evidence, the district court granted Bold’s well-supported motion for summary judgment. Dice, for the first time on appeal, cites record evidence that it claims supports a finding of misappropriation. We do not, however, “entertain on appeal factual recitations not presented to the district court any more readily than [we] will tolerate attempts to enlarge the record itself.” Guarino, 980 F.2d at 404. The district court did not err in rejecting Dice’s conclusory allegations of misappropriation in the face of competent evidence to the contrary. *See* Fed. R. Civ. P. 56(c).

2.

Dice also argues that its software is a trade secret. Specifically, Dice claims that Bold misappropriated its receiver drivers that take incoming signals and convert the data to Dice’s standard. Although Dice’s briefing on this claim is opaque, we are skeptical whether Dice raised this claim before the district court. Neither in the operative complaint nor in Dice’s response to Bold’s motion for summary judgment can we find a trade secret claim based on receiver drivers or software that performs that function. In Bold’s motion for summary judgment, Bold discussed only the ALSCHART as material potentially subject to trade secret protection. In response, Dice referred only to software that compiles information—a description consistent with the ALSCHART’s function and not the receiver drivers. The district court then treated the
Alschart file as the subject of Dice’s trade secret claim in its order granting summary judgment. Had the district court made so plain an error in failing to consider an entirely independent trade secret claim, we would expect Dice to mention that in its motions for reconsideration or indicative ruling. It did not.

Even if not forfeited for this reason, Dice’s claim is defective for two independent reasons. First, as discussed above, Dice failed to present competent evidence of misappropriation to the district court. Second, much like the Alschart claim, Dice has never put forward any evidence, let alone make the argument, that its receiver drivers are actually a trade secret. Other than a generalized explanation of what the receiver drivers do, Dice has failed to explain whether the receiver drivers derive economic value from their secrecy.

B.

Dice alleges that to undertake the extraction process, Bold created an unauthorized derivative work in violation of the Copyright Act, 17 U.S.C. § 106(2). 17 U.S.C. § 411(a) provides: “no civil action for infringement of the copyright in any United States work shall be instituted until preregistration or registration of the copyright claim has been made in accordance with this title.” In Reed Elsevier, Inc. v. Muchnick, the Supreme Court clarified that this requirement is a precondition to suit and not a jurisdictional rule. 559 U.S. 154, 161 (2010).

Dice did not seek copyright protection until after it filed suit.3 We do not decide whether late registration can cure this non-jurisdictional defect. See Positive Black Talk Inc. v. Cash Money Records, Inc., 394 F.3d 357, 365 (5th Cir. 2004), abrogated by Reed Elsevier, 559 U.S. at 157. Dice’s claim fails for a separate reason. Not all copying amounts to copyright

---

3Dice’s reliance on Coles v. Wonder, 283 F.3d 798, 801 (6th Cir. 2002), is misplaced. Coles stands for the unremarkable proposition that although an action for infringement cannot be enforced until § 411’s filing requirements have been satisfied, copyright protection extends retroactively to the time the artist creates the work. Id.
Nos. 12-2513, 13-1712  

_Dice v. Bold_

infringement.  _Feist Publ’ns, Inc. v. Rural Tel. Serv. Co._, 499 U.S. 340, 361 (1991).  Allowing that registration constitutes _prima facie_ evidence of the copyright’s validity, see 17 U.S.C. § 410(c), the plaintiff must still prove “that the defendant copied protectable elements of the work.”  _Lexmark Int’l, Inc. v. Static Control Components, Inc._, 387 F.3d 522, 534 (6th Cir. 2004); see also _Feist_, 499 U.S. at 361.  Only original material is subject to copyright protection and, even then, elements of a computer program dictated by practical realities may not be protectable.  _See Lexmark_, 387 F.3d at 535.

Dice has not attempted to demonstrate which aspects of its programs were protectable. Dice does not identify any original elements in its software and does not argue that the receiver drivers represent non-functional expression. Irrespective of how unique the Dice standard or its source code, the district court was right not to find a fact question on the basis only of Dice’s say-so. Dice attempts to explain its failure to produce any such evidence by pointing to the fact that Bold belatedly produced the File List document, which, according to Dice, finally allowed it to inspect Bold’s Extraction Program. But in its motion for reconsideration and in its motion for indicative ruling, Dice failed to identify the original and non-functional elements of its work. Instead, it provided hundreds of pages of incomprehensible computer code without explanation other than Clifford Dice’s claim that “Bold’s extraction program utilized Dice source code in the conversion process.”

---

4Dice does not make this argument. Moreover, at least at the time Dice filed suit, it was not entitled to this benefit of registration. And finally, Dice does not claim a copyright in the ALSCHART, only in its receiver drivers.
C.

Dice asserts on appeal that Bold violated the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a), because customers allowed Bold to use their passwords to login to the Dice servers through the “Go To Assist function.”

For two reasons this claim fails. First, Dice did not cite any evidence of circumvention of technological measures to the district court. The district court rejected Dice’s claim for this reason. Likewise on appeal, to the extent we are inclined to allow Dice to resurrect its argument, Dice cites no evidence. Second, Dice’s general theory before the district court was that Bold circumvented Dice’s attempts to encrypt its software. Dice now argues that Bold violated the DMCA because ESC Central improperly allowed Bold to use its passwords to login to the Dice software operating at the customer’s site through the Go To Assist function. This is a new argument not appropriately considered on appeal.

D.

Dice argues that the district court erred in dismissing its private cause of action under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. 1030(g).\(^5\) Generally, the CFAA protects against unauthorized computer access. Dice puts forward a complex claim of unauthorized access. It claims that, although ESC Central’s servers running Dice software were owned by ESC Central, they were connected to the Dice disaster recovery network at Dice’s office in Michigan. According to Dice, customer-owned servers, like the ESC Central server running the Dice software, were actually a branch of Dice’s network. This is because, when a Dice system is installed, Dice’s Michigan servers mirror its customers’ servers. Consequently, according to Dice, when Bold employees accessed ESC Central servers they necessarily accessed the Dice

\(^5\)Dice does not clarify under which subsection it brings its claims, but this is ultimately irrelevant.
disaster recovery network. This argument, like many before, was not fairly made to the district court.\textsuperscript{6}

Even assuming this claim were fairly raised, it would still fail. Liability under the CFAA requires a showing of intentional access. 18 U.S.C. § 1030(a)(2). Neither Narowski nor Condon was aware that performing a Go To Assist Function on ESC Central servers allowed access to Dice servers in Bay City, Michigan. Dice also does not explain how, even if the Go To Assist function allowed access to Dice servers, Condon or Narowski used the Go To Assist function to obtain Dice source code. See 18 U.S.C. § 1030(e)(6). Condon explains:

If permission is granted by the customer, the Go To Assist function allows me to view the computer screen of the customer from Bold’s Colorado office and to perform commands on the customer’s computer. . . . The result is the same as if I was at the customer’s office and the customer allowed me to sit at their computer terminal and view their computer screen. . . .

Using Go To Assist I was able to view ESC’s computer screens for the ESC server running Dice and the ESC server running Bold to help diagnose [a] discrepancy in the signal interpretations. As far as I am aware, the Go to Assist function would not allow myself or any other Bold user to access Dice source code in the Dice software running on ESC’s servers and I have never used Go To Assist for that purpose.”

And Narowski attested: “With GoToAssist I cannot access any Dice source code even if the Dice software is running on the customer’s computer which grants access and I have never used

\textsuperscript{6}Dice’s response to Bold’s motion for summary judgment stated: “gotoassist enabled Mr. Narowski and any other qualified Bold employee to access Dice servers without alerting Dice.” Dice did not explain that this occurred through the mirroring function of the disaster recovery network nor did Dice cite any evidence for that claim. On appeal, Dice points to the fact that in an affidavit attached as an exhibit, Clifford Dice explained the mirroring function. But the district court was not required to comb through the uncited record to make sense of Dice’s claim and, at the very least, Dice was obligated to explain the factual basis for its claim to the district court. See Tucker v. Tennessee, 539 F.3d 526, 531 (6th Cir. 2008).
GoToAssist to access any Dice source code.” As for Dice’s claim that Condon accessed Dice’s servers to acquire the ALSCHART file, Dice has not presented any evidence.

V.

For the foregoing reasons, we affirm the district court’s grant of Bold’s motion for summary judgment and its denial of Dice’s motion for indicative ruling.
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: GOOGLE INC. GMAIL LITIGATION

ORDER DENYING PLAINTIFFS’ MOTION FOR CLASS CERTIFICATION

THIS DOCUMENT RELATES TO:
ALL ACTIONS

In this consolidated multi-district litigation, Plaintiffs Keith Dunbar, Brad Scott, Todd Harrington, Ronald Kovler, Matthew Knowles, A.K. (next friend to Minor J.K.), Brent Matthew Scott, Robert Fread, and Rafael Carrillo, individually and on behalf of those similarly situated (collectively, “Plaintiffs”), allege that Defendant Google, Inc., has violated state and federal anti-wiretapping laws in its operation of Gmail, an email service. See ECF No. 98-4 (“FACC”). Pending before the Court is Plaintiffs’ Motion for Class Certification, in which Plaintiffs move to certify four Classes and three Subclasses. See ECF No. 87-26 (“Mot.”). Google has filed an Opposition, see ECF No. 101-2 (“Opp.”), and Plaintiffs have filed a Reply, see ECF No. 112-2 (“Reply”). The Court held a hearing on the Motion on February 27, 2014. See ECF No. 148 (“Tr.”). Having considered the briefing, the record in this case, and the oral arguments presented at the hearing, the Court DENIES Plaintiffs’ Motion for Class Certification.
I. BACKGROUND

A. Factual Background

Plaintiffs challenge Google’s operation of Gmail under state and federal anti-wiretapping laws. In the FACC, Plaintiffs seek damages, injunctive relief, and declaratory relief on behalf of a number of classes of individuals who either use Gmail or exchange messages with those who use Gmail for Google’s interception of emails over a period of several years. FACC ¶¶ 254-349.


1. Email Users Implicated

Google’s operation of Gmail implicates several different groups of email users, whose interactions with Google’s processes are slightly different. Accordingly, the Court begins by providing background on the types of email users implicated in this litigation and explaining the agreements with Google that each of these types of users encounter as they set up their email accounts.

First, Google provides a free web-based email service called Gmail. ECF No. 103-1, (“Chin Decl.”) ¶ 2. Users of this service can sign up for an “@gmail.com” account on a Google webpage, titled “Create an Account.” Id. ¶ 10. In the process of creating an account, users of Google’s free Gmail service (to whom the Court will refer as “Gmail users”) must check a box indicating that they agree to be bound by Google’s Terms of Service (“TOS”) and Privacy Policy. Id. ¶ 9. The “Create an Account” page links to webpages containing the relevant TOS and Privacy Policy. See id., Ex. F. Named Plaintiff J.K. went through this process to create the Gmail account at issue in the instant litigation. Id. ¶ 10.
Second, Google offers a service known as “Google Apps” to customers including businesses, educational organizations, and internet service providers (“ISPs”). Id. ¶ 3. Through Google Apps, these customers can provide Google services, including Gmail, Google Calendar, and Google Docs, to their employees, students, or customers (to whom the Court refers as “end users”). Id. The end users do not receive “@gmail.com” email addresses. Id. Rather, their email addresses contain the domain name of the entity that contracts with Google to provide the services. Id. The business or educational institution that contracts with Google for Google Apps (to whom the Court refers as “Google Apps Administrators”) is responsible for overseeing the creation of the accounts of end users. Id.

The instant litigation concerns two sets of Google Apps end users. The first set is comprised of end users of Cable One, an ISP that contracts with Google to provide Google Apps-related services to its customers. FACC ¶ 99. Cable One contracted with Google and agreed to ensure that its end users agreed to the Google Apps TOS, which are, in all respects relevant to the instant litigation, identical to the Gmail TOS. Id. Importantly, Google’s agreement with Cable One precludes Google from displaying advertisements in connection with the Google Apps services. ECF No. 86-16 (“Rommel Decl.”), Ex. Q ¶ 1.7. Named Plaintiff Keith Dunbar is a Cable One customer who seeks to represent a class of Cable One end users. FACC ¶ 8.

The second set of Google Apps end users in this litigation are Google Apps for Education users. Like Cable One, educational institutions that provide Google Apps services agreed, in their contracts with Google, to obtain the necessary authorization from end users to enable Google to provide the services. Chin Decl. ¶¶ 3-4. The contracts further required Google to comply with Google’s Privacy Policies. Id. ¶¶ 7-8. Moreover, like Cable One end users, Google Apps for Education end users also did not receive advertisements. FACC ¶ 244. Named Plaintiff Rafael Carrillo, who was a student of the University of the Pacific, and named Plaintiff Robert Fread, a student at the University of Hawaii, were end users of Google Apps for Education as a result of
those institutions’ use of Google Apps. *Id.* ¶¶ 223-44. Fread and Carrillo now seek to represent a
class of Google Apps for Education end users. *Id.* ¶ 13.

*Third,* Plaintiffs include individuals who do not use any of Google’s services, but are
nevertheless impacted by the interceptions because these individuals send emails to or receive
emails from Gmail users. *Id.* ¶¶ 251-53. The Court will refer to these individuals, whom named
Plaintiffs Brad Scott, Todd Harrington, Ronald Kovler, Matthew Knowles, and Brent Scott seek to
represent, as “non-Gmail users.” *Id.*

2. The Operation of Gmail and Accused Devices

Google’s processing of Gmail has changed twice during the class periods: in 2010
and 2011. FACC ¶¶ 39, 79. While Plaintiffs have accused various steps of the Gmail
processing of unlawful interceptions in their pleadings, they clarify the scope of their contentions
in their Reply in support of the instant Motion. Reply at 6. Specifically, Plaintiffs clarify that
Google’s processing of emails with respect to only two sets of email transmission is at issue. *Id.*

First, Plaintiffs are concerned with the processing of emails sent to Gmail users by putative Class
members who are Gmail users, Google Apps users, or non-Gmail users. *Id.* Second, Plaintiffs are
concerned with the processing of email messages received by putative Class members who are
Google Apps and Gmail users. *Id.* Plaintiffs clarify that these two sets of challenged interceptions
occur as a result of three devices that process Google’s emails: (1) Content Onebox (“COB”), (2)
Medley Server, and (3) Changeling. *Id.* n.18. Accordingly, Plaintiffs clarify that they are not
seeking to certify classes to accuse the CAT2 Mixer, which had previously been accused, of
unlawful interceptions.¹ *Id.*

With respect to Google’s processes before 2010, Plaintiffs contend that Google
used the CAT2 Mixer, Medley Server, and ICEbox Server to read the content of emails received by

¹ The CAT2 Mixer processes emails sent from an @gmail.com account, which Plaintiffs have not
challenged here, and also had a role in the processing of messages received by @gmail.com
accounts before 2010, as discussed in this section.
United States District Court
For the Northern District of California

@mailto.com email addresses for keywords. FACC ¶¶ 25-30. Plaintiffs contend that Google extracted concepts from the content of the emails. FACC ¶¶ 25-28; Mot. at 4. Moreover, Plaintiffs contend that Google acquired metadata from the content of the email messages, and that this metadata was stored in secret user profiles. FACC ¶¶ 73-78; Mot at 4, 6.

Between 2010 and 20 _, Plaintiffs contend that Google routed all emails received by Gmail users through the COB. FACC ¶ 39; Mot. at 4. Through the COB, Plaintiffs contend, Google acquired message content and meaning even when the user was not receiving a personalized advertisement. Id. The information that the COB extracted was used to create metadata and annotations, which are allegedly stored in secret user profiles. FACC ¶¶ 73-78; Mot at 5.

Finally, with respect to post-2010 processing, Plaintiffs contend that Google moved the COB. FACC ¶ 79; Mot. at 5-6.

3. Google’s Disclosures

Google points to a number of documents publically available through its various webpages that discuss the challenged interceptions at issue in the instant litigation to contend that its users were aware of the interceptions. While it is clear that Gmail users had to indicate that they read some of these disclosures as part of the account registration process, it is not clear from the record

---

2 In their Motion for Class Certification, Plaintiffs also suggest that transcribed phone calls through Google Voice are subject to COB processing. Mot. at 6. However, this theory appears nowhere in the FACC, and the Court therefore does not consider it here.
to which disclosures the two groups of Google Apps users were exposed in their account-registration process. Accordingly, the Court discusses disclosures to the two sets of Google Apps users separately below.

First, Google points to the TOS to which all Gmail users had to agree to create a Gmail account. Gmail users were alerted to the TOS when they created a Gmail account. Chin Decl. ¶ 9. The first TOS was in effect from April 16, 2007, to March 1, 2012; the second was in effect from March 1, 2012 to November 11, 2013; and a third has been in effect since November 11, 2013. Id. ¶¶ 14-15. The 2007 TOS stated that:

Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings . . . . In addition, there are commercially available services and software to limit access to material that you may find objectionable.

Chin Decl., Ex. G, ¶ 8.3. A subsequent section of the 2007 TOS provided that “[s]ome of the Services are supported by advertising revenue and may display advertisements and promotions” and that “[t]hese advertisements may be content-based to the content information stored on the Services, queries made through the Service or other information.” Id. ¶ 17.1

The 2012 TOS deleted all of the above language and stated that users “give Google (and those [Google] work[s] with) a worldwide license to use . . . , create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content.” Id., Ex. H. The 2013 TOS is, for purposes of the instant litigation, identical to the 2012 TOS. Id. ¶ 15 n.5.

our services to users, including the display of customized content and advertising.” Id. In 2010, Google updated the Policy to state that the collected information would be used to “[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services.” Id., Ex. K. Importantly, for all of these policies, under the heading of “User Communications,” which Google collected, Google stated that “[w]hen you send email or other communications to Google, we may retain those communications in order to process your inquiries, respond to your requests and improve our services.” Id., Exs. I-K. Google combined various product-specific Privacy Policies on March 1, 2012. The purpose of the combination was to allow Google to integrate user data collected from its various products.3 In that Privacy Policy, Google eliminated the “User Communications” from the enumerated list of types of data that Google said it collected. Id., Ex. L.

Third, the Privacy Policies in place from August 7, 2008 to March 1, 2012 also incorporated product-specific privacy notices, such as two Gmail Privacy Notices that were in place until October 3, 2010. Id. ¶ 20; id., Exs. M, N. The Gmail Privacy Notices stated that “Google records information such as account activity (including storage usage, number of log-ins), data displayed or clicked on (including UI [user interface] elements, ads, links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL).” Id. The Notices went on to state that “Google’s computers process the information in your messages for various purposes, including formatting and displaying the information to you, delivering advertisements and related links, preventing unsolicited bulk email (spam), backing up your messages, and other purposes relating to offering you Gmail.”4 Id.


4 Google cites again, as it did in connection with the Motion to Dismiss, a “Legal Notice” that states that “Google does not claim any ownership in any of the content, including any text, data, information, images, photographs, music, sound, video, or other material, that [users] upload, transmit or store in [their] Gmail account.” Chin Decl. ¶ 22; id., Ex. O. The Notice further stated...
Fourth, Google maintained a series of Help pages designed to provide users information on
various subjects. Id. ¶ 24. The first of these pages, which was accessible through a link on the
Create an Account” page that Gmail users utilized from June 2009 to June 2012, stated that “[i]n
Gmail, ads are related to the content of your messages” and that “[a]d targeting in Gmail is fully
automated and no humans read your email in order to target advertisements or related
information.” Id. ¶ 25; id., Ex. P. Another Help page, titled “More on Gmail and Privacy,” states
that “[e]mail messages remain strictly between the sender and intended recipients” except in certain
limited circumstances. Id., Ex. R. “These exceptions include requests by users that Google’s
support staff access their email message in order to diagnose problems; when Google is required by
law to do so; and when we are compelled to disclose personal information because we reasonably
believe it’s necessary in order to protect the rights, property or safety of Google, its users and the
public.” Id. The “More on Gmail and Privacy” Help page went on to state that “[i]n Gmail, users
will see text ads and links to related pages that are relevant to the content of their messages.” Id. A
third Help page, titled “Gmail, Security & Privacy,” states that “Gmail scans and processes all
messages using fully automated systems in order to do useful and innovative stuff like filter spam,
detect viruses and malware, show relevant ads, and develop and deliver new features across your
Google experience.” Id. ¶ 28. A fourth page, titled “Ads on Google search, Gmail, and certain other
Google websites,” states that “[w]hen we personalize ads, we display ads based on the contents of
all your emails.” Id. ¶ 30.

Fifth, Google maintained two other pages for short periods that contained information about
targeted advertising. The first, a page titled “Privacy Center” that was available from July 2011 to
June 2012, stated that “Google scans the text of Gmail messages in order to filter spam and detect
viruses. The Gmail filtering system also scans keywords in users’ email which are then used to
match and serve ads.” Id. ¶ 32. The second, a page titled “Your Data on Google: Advertising,”
that Google “will not use any of [users’] content for any purpose except to provide [users] with the
service.” Id., Ex. O.
which was available from October 2011 to February 2013, stated that “[i]n Gmail, ads are related to the content of your messages.” *Id.* ¶ 33.

*Sixth,* Google’s Ad Preferences Manager, which was launched in 2009, had a webpage for “Ads on Search and Gmail” that stated that “[w]ith personalized ads, we can improve your ad experience by showing you ads related to websites you visit, recent searches and clicks, or information from your Gmail inbox.” *Id.* ¶¶ 40, 42. Another webpage, “About Ads Settings” stated that “[t]he ads you see [in Gmail] may be based on many of the same factors as ads in Google Search as well as additional factors like the messages in your inbox.” *Id.* ¶ 43. The webpage provided an example: “You’ve recently received lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a local camera store.” *Id.*

*Seventh,* Google points to certain disclosures within the Gmail interface. *Id.* ¶ 54. Ads in Gmail are accompanied by a “Why this ad?” link, which when clicked displays a pop up that states that “[t]his ad is based on mails from your mailbox” and links to the Ads Preferences Managers discussed above. *Id.* ¶¶ 55-57. Moreover, from January 26, 2012 to March 1, 2012, Google advertised its new Privacy Policy on various Google websites and through a direct email to all Gmail users. *Id.* ¶¶ 48, 51. This email contained links to the TOS, Privacy Policy, Help pages, and Ad Preferences Manager. *Id.*, Ex. HH.

*Eighth,* Google cites blog posts and Securities and Exchange Commission (“SEC”) filings as additional disclosures of its alleged interceptions of emails. *Id.* ¶ 34. A January 20, 2010 blog post on the Official Gmail Blog informed users that “[w]hen you open a message in Gmail, you often see ads related to that email. Let’s say you’re looking at a confirmation email from a hotel in Chicago. Next to your email, you might see ads about flights to Chicago.” *Id.* ¶ 35. Moreover, Google cites one sentence of a more than one hundred page SEC filing, in which Google states that “[w]e serve small text ads that are relevant to the messages in Gmail.” *Id.* ¶ 36.
4. Disclosures to Cable One Users

As discussed above, Cable One contracted with Google and agreed to ensure that its end users agreed to the Google Apps TOS, which are, in all respects relevant to the instant litigation, identical to the 2007 Gmail TOS discussed above, which contained the language about Google’s ability to pre-screen or review content for objectionable material. *Id.* ¶ 6. However, it is not clear from the record that Cable One’s end users ever received a copy or link to the Google Apps TOS or that Cable One end users were required to agree to the TOS to create their accounts. That TOS states that “[b]y using Google’s products, software, services, or web sites . . . , you agree to the following terms and conditions, and any policies, guidelines, or amendments thereto that may be presented to you from time to time, including but not limited to Program Policies and Legal Notices . . . .” *Id.*, Ex. C. The TOS also incorporates by reference the Privacy Policy in effect at the time, by linking to Google’s Privacy Policy page, which contained the latest Privacy Policy. *Id.*

During the initial email migration process to Google Apps, Cable One provided users a link to the current version of the Google Privacy Policy (which contained the language that Google could collect “user communications . . . to Google”) at the bottom of the Account Transfer page. *Id.*, Ex. OO. After the migration to Google Apps, from 2010 to at least 2011, Cable One’s Self Support Portal page directed users interested in learning more about their email platform to Gmail Help pages. *Id.*, Ex. PP. The Gmail Help pages contain links to Google’s Privacy Policy and TOS at the bottom of the page. *Id.* The Self Support Portal also provided a link to “Legal Notices” at the bottom of the pages, but it is unclear from the record where the “Legal Notices” link leads. *Id.*

5. Educational Institutions’ Disclosures

As discussed above, the educational institutions with whom Google contracted were also required to obtain the necessary authorizations from end users for Google to provide its services. *Id.* ¶¶ 7-8. However, Google does not mandate how these educational institutions receive such authorizations, nor is that process uniform between various educational institutions. *Id.* ¶ 72. Accordingly, there are substantial differences between how each of the institutions approaches
disclosures. Moreover, it is unclear from the record what disclosures of the various universities each end user saw before registering for an account.

For example, for the University of the Pacific, the email sign-in page provides links to Google’s Privacy Policy and TOS at the bottom of the page, below the sign-in button. ECF No. 107 (“Wong Decl.”) ¶ 86. The University of Hawaii has a link to a Google Help Center to the side of the sign-in page. This Help Center contains links to Google’s TOS and Privacy Policy. Id. ¶ 87.

The Rochester Institute of Technology and Carnegie Mellon University direct users with questions regarding Google’s processing of email to Google’s Privacy Notices and Privacy Policies. Id. ¶ 89.

As discussed above, the specific language of the TOS, Privacy Policies, and Privacy Notices have evolved over the last five years, but these universities provide links to the latest versions on Google’s website. Therefore, some end users may have followed links from the universities to the TOS that contained the statement about Google’s authority to pre-screen material to prevent objectionable content, while others may have viewed the Privacy Policies’ discussion that Google was authorized to collect user communications to Google.

In contrast to the Google disclosures, some universities provide more detail to end users regarding the alleged interceptions at issue in the instant litigation. The University of California, Santa Cruz has a webpage titled “Security Information for Google Apps,” where the University provides links to Google’s TOS and Privacy Policies that were in effect at the time as discussed above. Id. ¶ 91. However, this webpage also contains a list of myths and facts about Gmail, one of which is particularly relevant here. Id., Ex. 82. The webpage states, “MYTH: Google accesses people’s email for marketing purposes” and “FACT: Google Apps for Education is ad-free for students, faculty, and staff. This means that your email is not processed by Google’s advertising systems.” Id. In contrast, the University of Alaska has a Google Mail FAQ page, which asks “I hear that Google reads my email. Is this true?” The answer states, “They do not ‘read’ your email per se. For use in targeted advertising on their other sites, and if your email is not encrypted, software (not a person) does scan your mail and compile keywords for advertising.” Id. ¶ 88.
Similarly, Western Piedmont Community College’s FAQ page states in response to the question “I’ve heard that Google scans the text in emails of Gmail accounts. Is that true?”: “Well, yes, but probably not in the way you might be thinking. Google does use software or a ‘bot’ to scan Gmail emails for key words for the purposes of targeted advertising. Google then places small, unobtrusive, and relevant text ads alongside your Gmail messages, similar to those on the side of Google search results pages. The matching of ads to content is a completely automated process performed by computers. No humans read your email to target the ads, and no email content or other personally identifiable information is ever provided to advertisers.” Id. ¶ 94. Stanford University’s FAQ page links to Google’s Privacy Policy and states that “[i]n order to provide essential core features for Stanford Alumni Email, Google runs completely automated scanning and indexing processes to offer spam filtering, anti-virus protection, and malware detection. Their systems also scan content to make sure Apps work better for users, enabling functionality like search in Gmail or Google Docs.” Id., Ex. 89.

6. Publicity Regarding Operation of Gmail

Google also points to media reports that discuss Google’s scanning of emails as potential disclosures to which Class members may have been exposed. Id. ¶ 4. The news reports about Google’s scanning practices fall broadly into four categories.

First, there was extensive media reporting of Gmail’s launch in 2004. Id. ¶¶ 12-26. Several of the articles noted that Google automatically scanned all emails for the purposes of providing targeted advertising related to the content of emails. Id. For example, a USA Today article from 2004 states that “Google’s computers automatically scan the body of messages for keywords used to tailor ads and match other information in its vast database.” Id., Ex. 4. A New York Times column stated that Google “said that its software would place ads in your incoming messages, relevant to their contents.” Id., Ex. 7. An article in the Chicago Tribune stated that “Google uses its AdSense software to read every word in every e-mail, and it then serves up related ads in the right margin.” Id., Ex. 11. Finally, a San Jose Mercury News article stated that “[t]he most controversial
aspect of the [Gmail] service will likely be the small text ads that Google will automatically place
in every e-mail message. Powered by the company’s AdSense program, the ads will be contextual,
meaning they will relate to keywords in the e-mail.” Wong Decl., Ex. 15.

Second, there was continued discussion in the media between 2005 and 2010 regarding
Google’s scanning practices. Id. ¶ 35. For example, a 2007 New York Times story about an
unrelated online phone start-up, leads with “[c]ompanies like Google scan their e-mail users’ in-
boxes to deliver ads related to those messages. Will people be as willing to let a company listen in
on their phone conversations to do the same?” Id., Ex. 30. Similarly, a 2008 NPR story reported
that “four years ago, when Google launched its ad-based Gmail, a lot of people were concerned
that Google would be scanning private email to sell targeted ads. Today, most people don’t seem to
mind so much and continue to use it.” Id., Ex. 34. A 2008 Washington Post article notes that
“[m]illions of people subject themselves to . . . intensive scrutiny when they use Google’s Gmail
service, which scans the text of each message to place more relevant ads.” Id., Ex. 35.

Third, there was news coverage of Google’s 2011 roll out of a new advertising system,
which allowed Google not only to present advertisements targeted to individual emails, but rather
allowed Google to present advertisements tailored to information about users that Google
aggregates over time. Id. ¶ 50. NBC News reported, for example, that “[w]hat if your email service
gradually learned from the emails you send and read so that it could show you ads which you might
actually be interested in? That’s exactly what Google will be doing soon.” Id., Ex. 46. Similarly,
PC World reported that “[f]or years, Gmail has been reading users’ e-mails to display relevant ads,
but soon it’ll go a step further by learning users’ habits.” Id., Ex. 47. A New York Times column
also reported on this shift, stating that “[l]ast month, Google also announced that it was trying to
make its ads even more ‘useful and relevant’ by scanning for ‘importance signals’ and recurring
topics within messages to better serve up appropriate advertising.”5 Id., Ex. 50.

5 Google also cites publicity surrounding its 2012 consolidation of various Privacy Policies
discussed above. Wong Decl. ¶¶ 60. However, coverage of this consolidation related principally to
Fourth, there has been media coverage of the instant litigation and related litigation. Id. ¶ 70. For example, an Associated Press article states that “[a] Pennsylvania woman has accused Google Inc. of illegal wiretapping for ‘intercepting’ emails she sent to Gmail accounts and publishing content-related ads. Her lawsuit echoes others filed around the country by class-action lawyers who say the practice violates wiretap laws in some states.” Id., Ex. 64. A CBS News article also reported on the instant litigation, stating that “[f]or years, Google’s computers have scanned the content of millions of Gmals—Google’s popular email service—in order to figure out what ads the user might respond to.” Id., Ex. 67.

B. Procedural History

1. Dunbar


Dunbar then filed a motion for class certification. After full briefing and a hearing on December 8, 2011, Judge Folsom denied Plaintiffs’ class certification motion without prejudice on March 16, 2012. See Dunbar I, ECF No. 156 (E.D. Tex. March 16, 2012). In the order denying class certification, Judge Folsom found that Dunbar had, on balance, satisfied the requirements of Rule 23(a): numerosity, commonality, typicality, and adequacy of class representative and class counsel. Id. at 10-16. However, Judge Folsom found that Dunbar’s proposed class, of all non-
Gmail users who had sent emails from their non-“@gmail.com” accounts to a Gmail or Cable One account, was not ascertainable, because the proposed class excluded “individuals . . . who seek actual damages and profits from Google.” Id. at 4. Judge Folsom found that this exclusion was not objective, and that accordingly, the class was not ascertainable. Id. at 9. Furthermore, Judge Folsom found that Dunbar’s class definition was deficient because users with non-“@gmail.com” accounts necessarily included Google Apps users. Id. Judge Folsom also found that Dunbar had not satisfied Rule 23(b)(3)’s superiority requirement because Dunbar had not presented an adequate trial plan. Id. at 16-20. Finally, Judge Folsom found that Dunbar had not satisfied the predominance requirement because there would be potential individualized questions of consent under Dunbar’s proposed trial plan. Id. at 21-22.

On April 20, 2012, one month after Judge Folsom’s class certification denial, Google filed another motion to dismiss, seeking dismissal on venue grounds. See Dunbar I, ECF No. 160 (E.D. Tex. April 20, 2012). In the alternative, Google requested that the case be transferred to the Northern District of California. See id. The motion to transfer was granted, and the case was transferred to this Court and assigned to the undersigned judge on June 27, 2012. See Dunbar v. Google, Inc. (“Dunbar II”), No. 12-3305, ECF No. 180 (N.D. Cal. July 23, 2012).

On August 28, 2012, Dunbar moved for leave to amend the complaint and indicated his intent to file a renewed class certification motion. See Dunbar II, ECF No. 205 (N.D. Cal. Aug. 28, 2012). After full briefing and a hearing, this Court granted the motion for leave to amend on December 12, 2012. See Dunbar II, ECF No. 226 (N.D. Cal. Dec. 12, 2012). The Court found that Dunbar had been diligent since Judge Folsom’s denial of the initial class certification motion, and that Google would not be unduly prejudiced by amendment because the Court would not reopen class discovery, which had closed on October 25, 2011. Id. at 17-25. Moreover, in the order on Dunbar’s motion for leave to amend, the Court extensively addressed Google’s contention that amendment would be futile because the amended complaint could not remedy the defects that Judge Folsom identified in his class certification order. Id. at 25-30. Specifically, the Court noted...
that the new class definition in the complaint did not exclude those who sought damages from
Google and that the new class definition focused on Cable One users rather than users with non-
“@gmail.com” addresses, which would encompass Google Apps users. Id. at 26-27. Moreover, the
Court noted that while predominance and superiority concerns may preclude class certification,
leave to amend should be granted because Judge Folsom’s denial of class certification was
explicitly without prejudice, suggesting that amendment and more evidence could cure the
deficiencies identified in Judge Folsom’s class certification order. Id. at 28-30. After this Court
granted leave, Plaintiff filed a Third Amended Complaint, which Google answered. See Dunbar II,

On January 8, 2013, this Court set a briefing schedule for Dunbar’s renewed class
certification motion. See Dunbar II, ECF No. 242 (N.D. Cal. Jan. 8, 2013). Pursuant to this
schedule, on January 28, 2013, Dunbar filed a renewed class certification motion. See Dunbar II,
ECF No. 249 (N.D. Cal. Jan. 28, 2013). In the motion, Dunbar sought to certify a class of Cable
One users who used their Cable One Google Apps email account to send a message to a Gmail user
or receive a message in the two years before the filing of Dunbar up until class certification. Id. at
6. On March 7, 2013, Google filed an opposition, contending that Dunbar could not show
predominance because individual issues of whether interceptions had taken place and individual
issues of consent would predominate over any common issues, that Dunbar was an inadequate
class representative, and that adjudication by class would not be superior to individualized
adjudications. See Dunbar II, ECF No. 261 (N.D. Cal. March 7, 2013). Dunbar filed his reply brief
on March 28, 2013, contending that both express and implied consent could be litigated on a class-
wide basis, that Dunbar is an adequate class representative, and that class adjudication would be
superior to individual actions. See Dunbar II, ECF No. 269 (N.D. Cal. March 28, 2013).

2. Other Cases and Consolidation

While Dunbar was pending, five other actions involving substantially similar allegations
against Google were filed in this District and throughout the country. See Scott, et al. v. Google,
United States District Court
For the Northern District of California

No. 12-6699 (E.D. Pa.). On April 1, 2013, before the Court could rule on Dunbar’s class
certification motion, the Judicial Panel on Multidistrict Litigation issued a Transfer Order,
centralizing Dunbar along with the five other actions in the Northern District of California before
the undersigned judge. See ECF No. 1. At an initial case management conference on April 18,
2013, the Court ordered Plaintiffs to file a consolidated complaint on May 16, 2013, set the
briefing schedule for any motion to dismiss, and scheduled a hearing for September 5, 2013. See
ECF No. 9. The Court also set a class certification briefing schedule and a class certification
hearing for January 16, 2014.7 See id. On May 6, 2013, this Court related a seventh action, Fread v.
Google, Inc., No. 13-1961 (N.D. Cal.), as part of this multi-district litigation. See ECF No. 29.

3. Motion to Dismiss and Motion to Certify

In line with the Court’s scheduling order, Plaintiffs filed a Consolidated Complaint on May
16, 2013. See ECF No. 38. That complaint attempted to state causes of action under (1) ECPA; (2)
CIPA; (3) Maryland’s Wiretap Act; (4) Florida’s Wiretap Act; and (5) Pennsylvania’s Wiretapping
to Dismiss the Consolidated Complaint on June 13, 2013. See ECF No. 44. After full briefing, this
Court held a hearing on the Motion to Dismiss on September 5, 2013. See ECF No. 64.

The Court issued an Order Granting in Part and Denying in Part the Motion to Dismiss on
September 26, 2013. See ECF No. 69. The Court granted Google’s Motion with respect to
Plaintiffs’ claims under section 632 of the California Penal Code, finding that emails were not
“confidential” under that part of CIPA. Id. at 40-42. The Court further found that Pennsylvania law
did not confer anti-wiretapping protections on recipients of emails and therefore granted Google’s
Motion with respect to the Pennsylvania law claims of non-Gmail users who merely received

7 The hearing was continued to February 27, 2014. See ECF No. 127.
emails from Gmail users. Id. at 42-43. The Court denied the rest of the Motion to Dismiss, rejecting Google’s two principal bases for dismissal. First, the Court rejected Google’s contention that any interceptions in the instant case fell within the “ordinary course” of Google’s business and were therefore exempt from anti-wiretapping statutes. Utilizing the tools of statutory interpretation, the Court concluded that the ordinary course of business exception was intended only to protect electronic communication service providers from liability where the interceptions helped facilitate or were instrumental to the provision of the electronic communication service. Id. at 19-20 ("In light of the statutory text, case law, statutory scheme, and legislative history concerning the ordinary course of business exception, the Court finds that the [‘ordinary course of business’] exception is narrow and designed only to protect electronic communication service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to provision of the electronic communication service at issue."). The Court further found that interceptions that violate an electronic communication service provider’s internal policies, as was alleged in the instant case, could not be within the provider’s ordinary course of business. Id. at 20-22. Second, the Court rejected Google’s argument that all Gmail users had consented to the alleged interceptions based on the TOS and Privacy Policy. The Court concluded that the TOS and Privacy Policy did not provide sufficient disclosures to conclude that Gmail users had consented to the alleged interceptions. Id. at 22-26. The Court further rejected Google’s contention that all email users, regardless of whether they had viewed any disclosures, had impliedly consented to the alleged interceptions, because all email users, including non-Gmail users, understand that such interceptions are part of how emails are transmitted. Id. at 27-28. The Court further held that Plaintiffs could proceed on their claims under section 631 of CIPA. Id. at 28-40.

On October 9, 2013, Google filed a Motion for § 1292(b) Certification for Interlocutory Review of this Court’s September 26, 2013 Order on the Motion to Dismiss. See ECF No. 80. Plaintiffs opposed that motion on October 16, 2013. See ECF No. 83. This Court held a hearing on the Section 1292(b) Certification Motion on October 29, 2013. See ECF No. 94. On January 27,
2014, the Court entered an Order denying Section 1292(b) Certification Motion, because the long and tortured history of the Dunbar action and the consolidated multi-district litigation suggested that immediate appeal would not materially advance the termination of the litigation. See ECF No. 129. Specifically, the Court found that Google’s desire to seek appellate review was belated, as Google did not seek appellate review of Judge Folsom’s May 23, 2011 order denying the initial motion to dismiss. Id. at 3. Moreover, the Court concluded that appellate review, years after the initial complaint was filed, would not prevent the parties from expending substantial resources as “multiple motions to dismiss have been fully briefed, argued, and ruled upon; multiple motions for class certification have been fully briefed; class discovery had closed in one of the cases more than two years ago; and fact discovery on the merits is set to close in less than three months.” Id. at 6. Finally, the Court agreed with Judge Folsom that regardless of where the precise line for the “ordinary course of business” exception was drawn, further factual development would be necessary and thus resolution of this issue was not appropriate on a motion to dismiss, which is limited to the four corners of the complaint. Id. at 6 n.2.

C. The Instant Motion

Plaintiffs filed the instant Motion for Class Certification on October 24, 2013. See Mot. In their Motion, Plaintiffs seek certification of the following four classes and three subclasses as described in the following chart:

<table>
<thead>
<tr>
<th>Class Definition</th>
<th>Class Reps.</th>
<th>Class Periods</th>
<th>Statutes at Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable One users who have, through their Cable One accounts, sent an email to an “@gmail.com” or “@cableone.com” email address or have received an email. (“Cable One Class”)</td>
<td>Dunbar</td>
<td>Two years prior to filing of the action to the date of certification.</td>
<td>Federal Wiretap Act</td>
</tr>
<tr>
<td>All Google Apps for Education users who have, through their Google Apps for Education accounts, sent an email to an “@gmail.com” address or have received an email. (“Education Class”)</td>
<td>Fread and Carrillo</td>
<td>Longest period allowed by statute of limitations to the date of certification.</td>
<td>Federal Wiretap Act</td>
</tr>
<tr>
<td>All Gmail users between the ages of thirteen and the age of majority (“minors”) who used their</td>
<td>A.K., as next of</td>
<td>Two years prior to filing of the</td>
<td>Federal Wiretap Act</td>
</tr>
</tbody>
</table>

Case No.: 13-MD-02430-LHK
ORDER DENYING PLAINTIFFS’ MOTION FOR CLASS CERTIFICATION
<table>
<thead>
<tr>
<th>Gmail accounts to send an email to a minor Gmail user or to receive an email from a non-Gmail user or a minor Gmail user. (“Minor Class”)</th>
<th>friend to minor J.K.</th>
<th>action to the date of certification.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All U.S. resident non-Gmail users who have used their non-Gmail accounts to receive an email from an “@gmail.com” address or to send an email message to an “@gmail.com” email address. (“Non-Gmail Wiretap Act Class”)</td>
<td>Kovler, Harrington, Brad Scott</td>
<td>Longest period allowed by statute of limitations to the date of certification.</td>
<td>Federal Wiretap Act</td>
</tr>
<tr>
<td>Subclass of Non-Gmail Wiretap Act Class: All U.S. residents, except California residents, who have used their non-Gmail accounts to send an email message to an “@gmail.com” email address. (“Non-Gmail CIPA Subclass”)</td>
<td>Kovler, Harrington, Brad Scott</td>
<td>Longest period allowed by statute of limitations to the date of certification.</td>
<td>CIPA</td>
</tr>
<tr>
<td>Subclass of Non-Gmail Wiretap Act Class: All Florida residents who have used their non-Gmail accounts to send an email message to an “@gmail.com” email address. (“Non-Gmail Florida Subclass”)</td>
<td>Brent Scott</td>
<td>Longest period allowed by statute of limitations to the date of certification.</td>
<td>Florida Statute §§ 934.03, et seq.</td>
</tr>
<tr>
<td>Subclass of Non-Gmail Wiretap Act Class: All Maryland residents who have used their non-Gmail accounts to send an email message to an “@gmail.com” email address. (“Non-Gmail Maryland Subclass”)</td>
<td>Knowles</td>
<td>Longest period allowed by statute of limitations to the date of certification.</td>
<td>Maryland Cts. and Judicial Proceedings Code §§ 10-402, et seq.</td>
</tr>
</tbody>
</table>

See Mot. at 9-10; Reply at 6 n.18; ECF No. 115. Excluded from all classes are all state, local, and federal government entities; individuals who timely opt out; current or former Google employees; individuals who have previously settled the claims identified in the FACC; and any currently sitting federal judge and people within three degrees of consanguinity to any federal judge. FACC ¶ 352. Defendants filed an Opposition to Plaintiffs’ Motion for Class Certification on November 21, 2013. See Opp. Plaintiffs filed a Reply in support of their Motion on December 19, 2013. See Reply. The Court held a hearing on February 27, 2014. See Tr.

 After the close of briefing, the parties filed motions to supplement the record. On February 6, 2014, Plaintiffs filed a Motion for Leave to Supplement the Record, which Google opposed. ECF Nos. 130-2, 134. Plaintiffs seek to introduce emails regarding the interceptions between named Plaintiff Fread and Google. The Court DENIES Plaintiff’s motion on the basis that the emails go to Fread’s individual concerns about the use of Google Apps services by the University of Hawaii and thus are not relevant to any issues of class certification. On February 25, 2014, Google filed a Motion to Supplement the Record with additional excerpts of a deposition of Plaintiffs’ expert, Dr. Matthew Green, who submitted a declaration in conjunction with the Reply in support of the
II. LEGAL STANDARD

Federal Rule of Civil Procedure 23, which governs class certification, has two sets of distinct requirements that Plaintiffs must meet before the Court may certify a class. Plaintiffs must meet all of the requirements of Rule 23(a) and must satisfy at least one of the prongs of Rule 23(b).

Under Rule 23(a), the Court may certify a class only where “(1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class.” Fed. R. Civ. P. 23(a). Courts refer to these four requirements, which must be satisfied to maintain a class action, as “numerosity, commonality, typicality and adequacy of representation.” Mazza v. Am. Honda Motor Co., 666 F.3d 581, 588 (9th Cir. 2012). Further, courts have implied an additional requirement under Rule 23(a): that the class to be certified be ascertainable. See Marcus v. BMW of North America, LLC, 687 F.3d 583, 592-93 (3d Cir. 2012); Herrera v. LCS Fin. Servs. Corp., 274 F.R.D. 666, 671-72 (N.D. Cal. 2011).

In addition to meeting the requirements of Rule 23(a), the Court must also find that Plaintiffs have satisfied “through evidentiary proof” one of the three subsections of Rule 23(b).

Comcast Corp. v. Behrend, 133 S. Ct. 1426, 1432 (2013). The Court can certify a Rule 23(b)(1) class when Plaintiffs make a showing that there would be a risk of substantial prejudice or inconsistent adjudications if there were separate adjudications. Fed. R. Civ. P. 23(b)(1). The Court can certify a Rule 23(b)(2) class if “the party opposing the class has acted or refused to act on instant Motion. See ECF No. 141. The Court GRANTED this motion, which Plaintiffs do not oppose, at the hearing. Tr. 7:20. Google also moved to file a Statement of Recent Decision regarding the Marin County Superior Court’s decision in Diamond v. Google, which Plaintiffs have opposed. See ECF Nos. 141-42. The Court DENIES Google’s motion because the reasoned tentative decision of the Marin County Superior Court was superseded by a two-sentence order on the motion that stated only that the Court’s rationale was placed on the record. On March 18, 2014, Plaintiffs filed another Motion to Supplement the Record. See ECF No. 156-2. The Court GRANTS this Motion because the material contained therein relates to the uniformity in Google’s processing of emails, which is relevant to class certification.
grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.” Fed. R. Civ. P. 23(b)(2). Finally, the Court can certify a Rule 23(b)(3) class if the Court finds that “questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b)(3) (emphasis added).

“[A] court’s class-certification analysis must be ‘rigorous’ and may ‘entail some overlap with the merits of the plaintiff’s underlying claim.’” Amgen Inc. v. Conn. Ret. Plans and Trust Funds, 133 S. Ct. 1184, 1194 (2013) (quoting Wal-Mart Stores, Inc. v. Dukes, 131 S. Ct. 2541, 2551 (2011)); see also Mazza, 666 F.3d at 588 (“Before certifying a class, the trial court must conduct a ‘rigorous analysis’ to determine whether the party seeking certification has met the prerequisites of Rule 23.”) (quoting Zinser v. Accufix Research Inst., Inc., 253 F.3d 1180, 1186, amended by 273 F.3d 1266 (9th Cir. 2001)). Nevertheless, “Rule 23 grants courts no license to engage in free-ranging merits inquiries at the certification stage.” Amgen, 133 S. Ct. at 1194-95.

“Merits questions may be considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied.” Id. at 1195. Within the framework of Rule 23, the Court ultimately has broad discretion over whether to certify a class. Zinser, 253 F.3d at 1186.

III. DISCUSSION

Plaintiffs move to certify all four Classes and three Subclasses identified above as Rule 23(b)(3) damages classes. Google does not challenge Plaintiffs’ position that the putative Classes meet the numerosity and commonality requirements. Instead, Google contends that none of the Classes satisfies the ascertainability, predominance, and superiority requirements. Google also challenges some of the Classes under choice of law principles and contends that some Classes cannot meet the adequacy and typicality requirements of Rule 23(a). The Court finds that none of the Classes can satisfy the predominance requirement. Accordingly, the Court does not reach
Google’s remaining contentions. The Court begins by setting forth the legal standard for predominance and then applies that standard to the four Classes and three Subclasses. After doing so, the Court concludes that individual issues regarding whether members of the various Classes consented to the alleged interceptions will predominate over common issues.

A. Legal Standard for Predominance

The predominance inquiry of Rule 23(b)(3) “tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation.” Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 623 (1997). Accordingly, the predominance analysis “focuses on the relationship between the common and individual issues in the case.” Wang v. Chinese Daily News, Inc., 737 F.3d 538, 545 (9th Cir. 2013) (internal quotation marks omitted); see also In re Wells Fargo Home Mortgage Overtime Pay Litig., 571 F.3d 953, 958 (9th Cir. 2009) (“Whether judicial economy will be served in a particular case turns on close scrutiny of the relationship between the common and individual issues.” (internal quotation marks omitted)).

Undertaking the predominance analysis requires some inquiry into the merits, as the Court must consider “how a trial on the merits would be conducted if a class were certified.” Gene And Gene LLC v. BioPay LLC, 541 F.3d 318, 326 (5th Cir. 2008); see also Zinser, 253 F.3d at 1190 (noting that district courts must consider as part of the predominance analysis whether a manageable class adjudication can be conducted). Though the Court needs to consider the merits to determine whether the action can be litigated on a class-wide basis, the Supreme Court has cautioned that class certification is not an opportunity for the Court to undertake plenary merits inquiries. As the Supreme Court has stated, “[m]erits questions may be considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied.” Amgen Inc., 133 S. Ct. at 1195; see also In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig., 722 F.3d 838, 851 (6th Cir. 2013) (noting that merits inquiries at the class certification stage are limited to those necessary to resolving the question presented by Rule 23).
The Court’s predominance analysis “entails identifying the substantive issues that will control the outcome, assessing which issues will predominate, and then determining whether the issues are common to the class, a process that ultimately prevents the class from degenerating into a series of individual trials.” *Gene And Gene LLC*, 541 F.3d at 326; see also *In re New Motor Vehicles Canadian Exp. Antitrust Litig.*, 522 F.3d 6, 20 (1st Cir. 2008) (“Under the predominance inquiry, a district court must formulate some prediction as to how specific issues will play out in order to determine whether common or individual issues predominate in a given case.” (internal quotation marks omitted)); *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1022 (9th Cir. 1998) (finding predominance “[w]hen common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication”). To meet the predominance requirement, “common questions must be a significant aspect of the case that can be resolved for all members of the class in a single adjudication.” *Berger v. Home Depot USA, Inc.*, 741 F.3d 1061, 1068 (9th Cir. 2014) (internal quotation marks and alterations omitted).

Importantly, the predominance inquiry is a pragmatic one, in which the Court does more than just count up common issues and individual issues. Wright & Miller, *Federal Practice & Procedure* § 1778 (3d ed. 2005) (noting that “the proper standard under Rule 23(b)(3) is a pragmatic one, which is in keeping with the basic objectives of the Rule 23(b)(3) class action”). As the Seventh Circuit recently stated, “predominance requires a qualitative assessment too; it is not bean counting.” *Butler v. Sears, Roebuck & Co.*, 727 F.3d 796, 801 (7th Cir. 2013). The Court’s inquiry is not whether common questions predominate with respect to individual elements or affirmative defenses; rather, the inquiry is a holistic one, in which the Court considers whether overall, considering the issues to be litigated, common issues will predominate. *Amgen*, 133 S. Ct. at 1196.

B. Application of the Predominance Standard

The Court now applies these standards to the four Classes and three Subclasses. The Court begins by describing the underlying merits inquiry before turning to the question of how best to
conduct such an inquiry. *Id.* at 1191 (“[T]he office of a Rule 23(b)(3) certification ruling is not to adjudicate the case; rather, it is to select the ‘metho[d]’ best suited to adjudication of the controversy ‘fairly and efficiently.’” (internal alterations omitted)).

The Wiretap Act, as amended by the ECPA, prohibits the interception of “wire, oral, or electronic communications.” 18 U.S.C. § 2511(1); *Joffe v. Google, Inc.*, No. 11-17483, 2013 WL 6905957, at *3 (9th Cir. Dec. 27, 2013). More specifically, the Wiretap Act provides a private right of action against any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of § 2511). The Wiretap Act contains several exemptions that render interceptions lawful. *See* 18 U.S.C. § 2511(2)(a)-(h). Among these exemptions is an exemption for consent:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.


The question of whether Class members have consented to the alleged interceptions has been central to this case since its inception. Specifically, the issue of whether email users consented to the alleged interceptions was at issue in all rounds of briefing on motions to dismiss, all three rounds of briefing on class certification, and the briefing on the motion for leave to amend. *See* [9 The distinction between one-party consent and two-party consent is immaterial to the Court’s analysis, because as discussed below, the issue of whether any email user (Gmail user, Google Apps end user, or non-Gmail user) consented to the alleged interceptions is a question fraught with individualized inquiries.]

---

9 The distinction between one-party consent and two-party consent is immaterial to the Court’s analysis, because as discussed below, the issue of whether any email user (Gmail user, Google Apps end user, or non-Gmail user) consented to the alleged interceptions is a question fraught with individualized inquiries.
In the briefs, the parties dispute whether the question of whether emails were intercepted pursuant to the Wiretap Act is a common question or an individual question. See Mot. at 18-20; Opp. at 18-22; Reply at 6-9. Plaintiffs contend that Google uniformly intercepts emails for COB processing. Google notes that there are a number of situations in which emails are not subject to COB processing. Opp. at 18-19. Only one of these situations—Google claims that Google Apps Administrators can configure their systems to avoid COB processing—would lead to individualized inquiries. Google relies exclusively on a declaration from a Google engineer for Google’s claim that Google Apps Administrators can avoid COB processing. See ECF No. 106 (“Long Decl.”) ¶ 3. Plaintiffs contend that this declaration contradicts the engineer’s previous deposition and Google’s recent representations to the media, and that therefore the declaration is a sham. Green Reply Decl. ¶ 10; ECF No. 156-2. The Court need not decide the question of whether the declaration is valid and therefore whether the question of interceptions is a class-wide question, because the Court finds that even if this question were a class-wide question, that common questions would be overwhelmed by individualized questions of consent as discussed below.
2511(2)(d). Therefore, the ultimate merits inquiry requires not only consideration of whether the Class members consented, but also whether their correspondents consented.\textsuperscript{11} However, for the three state statutes at issue with respect to the three Subclasses, the merits inquiry requires both parties to consent. Accordingly, if either party to a communication did not consent, that would end the inquiry.

In the instant litigation, Google has marshaled both express and implied theories of consent. Accordingly, the Court turns to each of the two theories of consent and describes the legal standard that must be applied with respect to each, the Court’s rulings regarding the two theories of consent at the Motion to Dismiss stage, and the evidence in the record that the parties will marshal going forward to prove the existence or absence of consent. The Court concludes, for the reasons stated below, that this evidence suggests that consent must be litigated on an individual, rather than class-wide basis. The Court will conclude by addressing Plaintiffs’ contentions to the contrary.

\textbf{1. Express Consent}

Courts have consistently noted that individuals may expressly consent to the interception of their communications. \textit{Pharmatrak}, 329 F.3d at 19; \textit{Van Poyck}, 77 F.3d at 292; \textit{United States v. Amen}, 831 F.2d 373, 378 (2d Cir. 1987). However, detailed discussion of the express consent exception to the Wiretap Act in the case law is relatively scant. Nevertheless, at the Motion to Dismiss stage, Google contended that Gmail users and all Google Apps end users had expressly consented to Google’s alleged interceptions. For this proposition, Google relied on the various

\textsuperscript{11} The Court does not separately discuss Minor Class members’ consent for four reasons. First, the parties have cited no case law suggesting that minors cannot provide consent to interceptions of their communications under the Wiretap Act. Second, Plaintiffs rely exclusively on a California statute, Cal. Fam. Code § 6701, to contend that minors cannot consent. However, this provision relates to contract law. As discussed below, consent for purposes of contract law is distinct from consent for purposes of the Wiretap Act. Third, even if state contract law consent principles were to negate a minor’s ability to consent under the Wiretap Act, there would be individual questions as to where the minor email senders and recipients reside and which state laws should apply. The nationwide Minor Class would therefore require several individual inquiries even under Plaintiffs’ theory. Fourth, to the extent that minors have corresponded with adults, there would be several individualized issues regarding the adult correspondent’s consent, as discussed below.
TOS and Privacy Policies that were in effect between 2008 and 2013. In the Order on the Motion to Dismiss, this Court rejected Google’s contentions. The Court held that the TOS and Privacy Policies did not provide sufficient disclosures regarding the alleged interceptions—the scanning of emails for the purposes of providing targeted advertising and creation of user profiles—to warrant dismissal under the express consent exception to the Wiretap Act. ECF No. 69 at 24-26.

Specifically, the Court found that Google’s reliance on the language of its TOS, which stated that “Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service,” was misplaced because that provision related to Google’s participation in the email delivery process to preclude objectionable content, particularly in light of the sentence that followed, which stated that “[f]or some of the Services, Google may provide tools to filter out explicit sexual content.” *Id.* at 24.

Similarly, the Court was not persuaded that the Privacy Policies, which stated that Google collected “[i]nformation you provide, [c]ookies[,] [l]og information[,] [u]ser communications . . . to Google[,] [a]ffiliated sites, [l]inks[,] [a]nd [o]ther sites” and used such information for the purposes of “[p]roviding our services to users, including the display of customized content and advertising,” provided clear enough disclosures regarding Google’s interceptions of emails between users to provide targeted advertisements. *Id.* at 25. In fact, the Court found that certain statements in the Privacy Policies, which stated that Google would collect “user communications . . . to Google” could actively obscure Google’s interceptions. *Id.* at 25-26 (emphasis in original).

At the instant stage of litigation, the Court must consider whether express consent is an issue that can be decided on a class-wide basis or whether individual issues will predominate. The Court notes that the question of express consent is usually a question of fact, where a fact-finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals regarding the interceptions. *See Murray v. Fin. Visions, Inc.*, No. 07-2578, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008).
Plaintiffs contend that the question of express consent is a question particularly susceptible to class-wide adjudication, since all Gmail users were subject to the same disclosures. While the Court agrees that express consent may be a common question with respect to the Minor Class and the Cable One Class, the express consent of Education Class members is likely to require individualized inquiries. This is so because Google had no single policy that required all Google Apps Administrators to provide the same disclosures to end users. See Chin Decl. ¶ 3. This means that the end users received vastly different disclosures depending on which educational institution they were affiliated. Some institutions’ disclosures are quite explicit. For example, Western Piedmont Community College tells its users that “Google does use software or a ‘bot’ to scan Gmail emails for key words for the purposes of targeted advertising.” Wong Decl., Ex. 85. Similarly, the University of Alaska states that “For use in targeted advertising on [Google’s] other sites, and if your email is not encrypted, software (not a person) does scan your mail and compile keywords for advertising.” Id., Ex. 79. Meanwhile, other universities, such as the University of the Pacific, merely incorporate Google’s disclosures by citing to the TOS and Privacy Policies. Id., Ex. 74. As discussed above, it is not clear that end users even had to look at these disclosures before they could create their accounts. Further, even if the users had seen these disclosures, as this Court noted above and in its Order on the Motion to Dismiss, Google’s disclosures were vague at best, and misleading, at worst. For example, the TOS stated only that Google retained authority to pre-screen content to prevent objectionable material, while the Privacy Policies suggested only that Google would collect user communications to Google. Accordingly, the diversity of disclosures made by educational institutions, ranging from specific disclosures about the method and reasons for interceptions to the incorporation of vague disclosures, may well lead a fact-finder to conclude that end users at some universities consented, while end users at other universities did not. As such, the Court finds that there are substantial individualized inquiries on the issue of express consent.

In sum, the Court finds that with respect to the Education Class, the substantial individual questions regarding the nature of each Google Apps Administrator’s disclosures are likely to lead
to individual questions regarding express consent that will predominate over common questions.

The Court need not determine whether class-wide express consent questions will predominate over individual questions with respect to the Minor Class, Cable One Class, and the Non-Gmail User Classes because, as discussed below, the Court finds that individualized questions regarding implied consent will overwhelm any common issues regarding these Classes.

2. **Implied Consent**

The Court now turns to implied consent. Implied consent is an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (“It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent.”); *see also Murray*, 2008 WL 4850328, at *4 (“The question of consent, either express or implied, is often a fact-intensive inquiry and may vary with the circumstances of the parties.”). As the D.C. Circuit has concluded, “[w]ithout actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception.” *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation marks and alterations omitted; emphasis added); *Van Poyck*, 77 F.3d at 292 (“Consent may be express or may be implied in fact from surrounding circumstances indicating that the defendant knowingly agreed to the surveillance.” (internal quotation marks and alterations omitted; emphasis added)). “[I]mplied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.” *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) (internal alterations and quotation marks omitted).

Applying this standard to the Motion to Dismiss, which examines only the four corners of the complaint, the Court rejected Google’s contention that the Court should conclude that all email users impliedly consented to Google’s interceptions on the basis of the Complaint alone, because
all email users understand that such interceptions are part and parcel of the email delivery process. ECF No. 69 at 27. The Court found that there was no authority to support Google’s “far-reaching proposition” that consent could be implied so broadly as a matter of law without any factual development. \textit{Id.} The Court therefore concluded that accepting Google’s theory of implied consent “would eviscerate the rule against interception” since under Google’s theory, consent could easily be implied as a matter of law with respect to large swaths of electronic communication services. \textit{Id.}

Now, at the class certification stage, the Court must consider what evidence Google can use to argue to the finder of fact that email users have impliedly consented to these interceptions. Google contends that a broad swath of evidence that email users were notified of the interceptions, such as Google disclosures, third-party disclosures, and news articles, are relevant to the factual question of implied consent. Plaintiffs contend that only Google’s own disclosures to its users are relevant to the question of implied consent.

The Court agrees with Google. As discussed above, courts have consistently held that implied consent is a question of fact that requires looking at all of the circumstances surrounding the interceptions to determine whether an individual knew that her communications were being intercepted. For example, the First Circuit has suggested that whether a party has impliedly consented is a factual question that requires a close examination of all the circumstances:

\textit{The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of [the Wiretap Act]—a purpose which suggests that consent should not casually be inferred. Griggs-Ryan, 904 F.2d at 117. Accordingly, “consent can be limited based upon the ‘subtleties and permutations inherent in a particular set of facts.’” Shefts v. Petrakis, 758 F. Supp. 2d 620, 631 (C.D. Ill. 2010) (quoting \textit{Griggs-Ryan}, 904 F.2d at 119).}

\textit{Amen} is instructive. There, the Second Circuit found that the consent exception to the Wiretap Act applied in the context of inmates whose phone calls were recorded. \textit{Amen}, 831 F.2d at
378-79. The Second Circuit found that consent could be implied, because the inmates were on
notice from several sources that their phone calls were being recorded. *Id.* at 379. The Second
Circuit found implied consent based on the following: (1) the taping system was discussed at
inmates’ orientation; (2) inmates received a handbook that discusses the interceptions; (3) there
were notices near the phone alerting inmates of the monitoring; and (4) one of the inmate’s case
managers presented the inmate with a form containing a written notice of disclosures, which the
inmate refused to sign. *Id.* The Second Circuit’s reliance on a form that the inmate did not sign, but
nevertheless saw, indicates that all materials to which an individual has notice are relevant to
consent, not just contractual agreements. *See Van Poyck,* 77 F.3d at 292 (approvingly citing *Amen*).

The First Circuit’s decision in *Williams v. Poulos,* 11 F.3d 271 (1st Cir. 1993), is in accord.
There, the First Circuit affirmed a district court’s finding, after a bench trial, that the CEO of a
company had not consented to interceptions of his telephone calls by his employer. *Id.* at 281-82.
The First Circuit noted that though the CEO was informed that the company had a system for
randomly monitoring calls, it was not clear whether the CEO knew “(1) of the manner—i.e., the
intercepting and recording of telephone conversations—in which this monitoring was conducted;
and (2) that he himself would be subjected to such monitoring.” *Id.* at 281. The First Circuit
concluded:

> There was testimony tending to indicate that [the CEO] was so informed, which the
district judge apparently chose not to credit, and testimony tending to indicate that
he was not. In our view, the latter testimony, far from being incredible, was highly
plausible. Thus, there is no basis for us to conclude that the district court clearly
erred in finding that [the CEO] was not told of the manner in which the monitoring
was conducted and that he himself would be monitored.

*Id.* at 281-82. The First Circuit, though ultimately rejecting the testimony, found that testimony
about what the CEO knew was relevant to whether the CEO had consented. The First Circuit could
have rejected the company’s contentions out of hand by requiring official or written notice. Rather,
the First Circuit found that the question of implied consent was fundamentally a factual question on
which all the testimony regarding what the CEO knew was relevant. In light of these authorities,
the Court concludes that while consent may only be implied in a narrow set of circumstances, a
broad set of materials are relevant to determining whether such consent should be implied.

Applying these legal principles here, the Court finds that individual issues regarding
consent are likely to overwhelmingly predominate over common issues. Specifically, there is a
panoply of sources from which email users could have learned of Google’s interceptions other than
Google’s TOS and Privacy Policies. First, Class members could have learned of the interceptions
from various Google sources. For example, the “About Ads on Search, Gmail and across the web”
page, which has been viewed more than a million times, states that “[t]he ads you see [in Gmail]
may be based on many of the same factors as ads in Google Search as well as additional factors
like the messages in your mailbox” and provides the following example: “You’ve recently received
lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a
local camera store.” Chin Decl. ¶¶ 41, 43; id., Ex. DD. Furthermore, the link for “Why This Ad?”
next to each targeted advertisement in Gmail, which led users to the disclosure that “[t]his ad is
based on emails from your inbox,” was clicked thousands of times in every day. Id. ¶ 56; id., Ex.
JJ. Second, Class members may have learned about the alleged interceptions from various media
sources. For example, a 2004 Houston Chronicle article states that “some industry watchers have
complained that Google scans account holders’ messages for keywords and then delivers text-
based ads relevant to the keywords detected. However, most Gmail users said they’re not bothered
by it.” Wong Decl., Ex. 13. Along a similar note, a Washington Post article stated, “Google’s
Gmail service has generated some controversy among privacy activists for the way its technology
serves up text ads to users based on the content of their messages. None of the Gmail account

12 Plaintiffs contend that these third-party documents are impermissible hearsay. See Reply at 5
n.15. However, Google does not cite this material for the truth of the matter asserted therein—that
is, to establish that Google actually intercepted emails. Rather, these documents are cited for the
effect on the listener—that is, to show that Plaintiffs had knowledge that Google engaged in
interceptions. United States v. Payne, 944 F.2d 1458, 1472 (9th Cir. 1991).
holders or would-be account holders contacted for this article expressed concerns along these lines.” *Id.*, Ex. 9.

Some Class members likely viewed some of these Google and non-Google disclosures, but others likely did not. A fact-finder, in determining whether Class members impliedly consented, would have to evaluate to which of the various sources each individual user had been exposed and whether each individual “knew about and consented to the interception” based on the sources to which she was exposed. *See Berry*, 146 F.3d at 1011. This fact-intensive inquiry will require individual inquiries into the knowledge of individual users. Such inquiries—determining to what disclosures each Class member was privy and determining whether that specific combination of disclosures was sufficient to imply consent—will lead to numerous individualized inquiries that will overwhelm any common questions.

### 3. Plaintiffs’ Contentions

Plaintiffs make three arguments in support of their claim that consent can be determined on a class-wide basis. First, Plaintiffs contend that in determining whether Gmail users impliedly consented, the finder of fact should be limited to looking at a uniform set of Google’s own disclosures, rather than to disclosures of third parties. Second, Plaintiffs contend that the parol evidence rule precludes the finder of fact from looking outside the contractual agreements between Gmail users and Google. Third, Plaintiffs contend that the specific disclosures to which Google points do not demonstrate consent, because those disclosures pre-date Google’s shift in email delivery processing from the CAT2 Mixer (which scanned emails only when the emails were opened) to COB (which scans all emails while the emails are in transit). In essence, Plaintiffs’ contention is that the third-party disclosures on which Google relies cannot disclose interceptions that did not exist at the time of the third-party disclosures.13 The Court does not find any of these contentions persuasive for the reasons stated below.

13 Plaintiffs also contend that consent can be negated on the basis that Google’s interceptions were for the “purpose of committing [a] . . . tortious act in violation of the . . . laws of the United States
First, Plaintiffs contend that the factual inquiry with respect to implied consent should be limited to looking at the disclosures that Google itself made, rather than disclosures that third parties, such as news media, made. Even if Plaintiffs were correct regarding the scope of documents to which a fact-finder could look, there would be a myriad of individual issues with respect to consent, because Google itself had several disclosures, which could not have been uniformly viewed by Class members. For example, as discussed above, a Google page titled “About Ads on Search, Gmail and across the web” stated that “[t]he ads you see [in Gmail] may be based on many of the same factors as ads in Google Search as well as additional factors like the messages in your inbox,” and provided the following example: “You’ve recently received lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a local camera store.” Chin Decl. ¶ 43, id., Ex. DD. It is undisputed that this page has been viewed more than 1.6 million times since July 2012. Id. A finder of fact could conclude that Class members who viewed this particular disclosure were on notice of the alleged interceptions. Similarly, some Class members may have been part of the 100,000 individuals who clicked the “Why This Ad?” link next to a content-based advertisement in a single day. Id. ¶ 58. Those users would have received a notice that “[t]his ad is based on emails from your inbox,” which again, a fact-finder could find sufficient to imply consent. Id., Ex. JJ. In light Google’s own disclosures’ diversity, even accepting

or any State,” 18 U.S.C. § 2511(2)(d), and that this is a class-wide question. Mot. at 23-24. Google responds that Plaintiffs have failed to allege or provide any evidence that Google acted with the wrongful intent necessary to fall within the tort or crime exception to the consent exception. Opp. at 17. The Court agrees with Google. Alleged interceptions fall within the tort or crime exception only where the “primary motivation or a determining factor in [the interceptor’s] actions has been to injure plaintiffs tortiously.” In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 518 (S.D.N.Y. 2001) (internal quotation marks omitted). Nothing in the FACC, the briefing on the instant Motion, or the record suggests that this is Google’s motivation here. Moreover, as the DoubleClick Court found in a different context, the tort or crime exception cannot apply where the interceptor’s “purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.” Id. The same is true here. Accordingly, the tort or crime exception to the consent exception will be unavailing for Plaintiffs to show absence of consent. Therefore, individualized inquiries will be needed to determine what each Class member knew.

35

Case No.: 13-MD-02430-LHK
ORDER DENYING PLAINTIFFS’ MOTION FOR CLASS CERTIFICATION
Plaintiffs’ theory, a fact-finder would have to evaluate whether consent could be implied from the specific set of Google disclosures that each individual user encountered.

Second, the Court also sees no basis as to why the disclosures relevant to a fact-finder’s determination of implied consent should be limited exclusively to Google disclosures. As discussed above, courts have held that the question of implied consent turns on whether the party whose communications were intercepted had notice of the interception or consented to the interception based on all of the surrounding circumstances. *Berry*, 146 F.3d at 1011; *Griggs-Ryan*, 904 F.2d at 117; *Amen*, 831 F.2d at 378. Plaintiffs do not cite any authority limiting the sources from which such notice or knowledge can be acquired, nor could this Court find such authority. Accordingly, the Court concludes that the full panoply of disclosures, from the news media, from Google, and from other sources, is relevant to the question of whether consent to the alleged interceptions should be implied from the surrounding circumstances. Plaintiffs contend that relying on extrinsic evidence outside of Google’s agreements with Class members would violate the parol evidence rule or that consideration of such evidence would be prohibited by the merger clause in the TOS.

While these could be valid contentions if Plaintiffs stated a breach of contract cause of action, these are not viable arguments with respect to the consent under the Wiretap Act, which requires the fact-finder to consider all the surrounding circumstances to determine whether an individual knew that her communications would be intercepted. *Amen*, 831 F.2d at 378 (holding that the critical question with respect to implied consent is whether consent can be implied “in fact from surrounding circumstances indicating that the [plaintiffs] knowingly agreed to the surveillance”).

Plaintiffs rely exclusively on a Northern District of Illinois case, *Harris v. comScore, Inc.*, 292 F.R.D. 579, 585 (N.D. Ill. 2013), for their proposition regarding the parol evidence rule. The Court, however, finds *Harris* unpersuasive. The *Harris* court held that “ComScore [the intercepting entity] contends that the scope of consent will vary for each plaintiff depending on his subjective understanding of the agreement and the surrounding circumstances. In support, comScore notes that at least under the ECPA, consent need not be explicit, but can also be implied from the
surrounding circumstances. But that rule has no place where a party manifested consent through the adoption of a form contract.” *Harris*, 292 F.R.D. at 585 (internal citations omitted). For the proposition in the last sentence, however, *Harris* merely cited a Seventh Circuit case interpreting Illinois contract law. The *Harris* court did not address the long line of cases that suggest a broader swath of materials is relevant to implied consent under the Wiretap Act. This Court concludes that unlike Illinois contract law, under which the subjective intent of the parties must give way to the terms of the contract that embody the parties’ mutual assent, see *Nat’l Prod. Workers Union Ins. Trust v. Cigna Corp.*, 665 F.3d 897, 901 (7th Cir. 2011), the question of implied consent to interceptions prohibited by the Wiretap Act necessarily requires an inquiry into what the party whose communications were intercepted subjectively understood.

Moreover, *Harris*, even if applicable, is distinguishable. In *Harris*, the user had a direct contract with the service provider, in which the user must have agreed to the user licensing agreement before she could use the software that engaged in the alleged interceptions. *Id.* at 582 (“The consumer must check either ‘Accept’ or ‘Decline’ before he may click ‘Next’ to proceed with downloading the free digital product. OSSProxy will download and install on the consumer's computer only if the consumer checks ‘Accept.’” (internal citations omitted)). In contrast, here, neither the Cable One nor Education Class members (who are end users) had any direct contractual relationship with Google. Moreover, in *Harris*, unlike this case, there were no potential other sources of disclosure, such as news articles, to which Class members in the instant litigation could have been exposed.

Furthermore, Plaintiffs’ contention that a finder of fact may only look to the agreements between Google and its users in determining consent improperly collapses express and implied consent. The agreements between Google and its users define the scope of the universe of material that the Court may consider in determining whether Plaintiffs have *expressly consented*. If the fact-finder were limited to the same material for purposes of determining implied consent, then express and implied consent would be coterminous. Courts have recognized, however, that express and
implied consent are analytically distinct. *Berry*, 146 F.3d at 1011 (noting that even “*without actual notice,*” consent can be implied “when the surrounding circumstances convincingly show that the party knew about and consented to the interception” (emphasis added; internal citations and alterations omitted)). It is only logical, in light of this recognition, for a finder of fact to be allowed to consider a broader set of materials in answering the factual question of whether users impliedly consented to the interceptions.14

Finally, Plaintiffs raised a new theory at the hearing on the instant Motion to contend that consent was a common question. Specifically, Plaintiffs contended that the existence of various third-party disclosures is irrelevant, because these disclosures could not have alerted Class members to the method of interceptions. Plaintiffs rely on the fact that in 2010, the Google device that intercepted emails shifted from the CAT2 Mixer, to the COB, which scans all emails. Plaintiffs contend that the pre-2010 third-party disclosures could have only alerted Class members about CAT2’s processing, not COB’s.

The Court is not persuaded. To find implied consent, a fact-finder need not determine email users had specific knowledge of the particular devices that intercepted their emails. Rather, the fact-finder need only be convinced based on the surrounding circumstances that email users were notified of interceptions. *Berry*, 146 F.3d at 1011 (noting that “[t]he key question in [the implied consent] inquiry obviously is whether parties were given sufficient notice” of the interceptions). To be relevant to this factual inquiry, a disclosure does not need to provide the specific devices at

14 Plaintiffs’ reliance on the deposition testimony of Google’s 30(b)(6) witness on consent, Aaron Rothman, is misplaced. Plaintiffs rely on Mr. Rothman’s testimony in response to counsel’s question regarding how an average user would know that Google interprets words in emails for meaning that “it is very clear in—in the multitude of documents provided by Google.” Mot. at 21 (citing Rommel Decl., Ex. I (“Rothman Depo.”) at 298). Plaintiffs overread Mr. Rothman’s testimony. In that part of Mr. Rothman’s testimony, he was merely contending that Google’s policies are sufficient to establish express consent. He was not, as Plaintiffs suggest, contending that the documents provided by Google were the sole sources from which users could learn of Google’s alleged interceptions.
issue. Griggs-Ryan, 904 F.2d at 117 (“The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private.”). Rather, a fact-finder could find implied consent even based on broad disclosures. Therefore, the Court finds that Google may rely on news articles to argue to the finder of fact that users impliedly consented, even if those news articles do not recite the specific devices that are alleged to have intercepted Class members’ emails.

Even if the Court were to accept Plaintiffs’ contention that the pre-2010 disclosures could not have alerted users to COB processing, which did not exist at that point, the Court would still conclude that individualized questions predominate with respect to consent because of the panoply of post-2010 disclosures that could be found to have put Class members on notice. For example, a 2012 Wall Street Journal article regarding Google’s consolidation of Privacy Policies informed users that “you may have noticed ads in your Gmail based on emails you had typed. Those appear because Google scans the content of emails for things like keywords that may be relevant for advertising.” Wong Decl., Ex. 53. Similarly, an October 22, 2012, New York Times article about Microsoft’s privacy policies states that “[t]he Microsoft policy appeared to give the company the same rights as Google, which scans the content of e-mails sent through its Gmail system, focusing on keywords to generate advertising that it thinks will interest the user.” Id., Ex. 55. Therefore, even if pre-2010 disclosures were not relevant to the implied consent inquiry, the Court would conclude that the post-2010 disclosures give rise to numerous individual inquiries regarding individual Class members’ knowledge of the interceptions. Plaintiffs’ sole contention with respect to these post-2010 disclosures is that these disclosures could not have disclosed COB processing, because Google has stated that the operation of the COB is a trade secret. The Court finds, however, that even if these disclosures did not specifically name COB processing, a fact-finder could conclude that these disclosures are sufficient surrounding circumstances to imply that email users “knowingly agreed
to the surveillance,” that is, the interceptions of their emails for purposes of targeted advertisements and user profiles. *Amen*, 831 F.2d at 378.

C. Conclusion Regarding Predominance

In sum, the Court finds that a fact-finder would have to determine to what disclosures each Class member was exposed and whether such disclosures were sufficient to conclude, under the Wiretap Act, that Class members consented to the alleged Google interceptions of email. This factual inquiry is an intensely individualized one. Furthermore, the myriad disclosures among the various Google Apps for Education Administrators raise a variety of individualized questions regarding express consent for the Education Class. The individualized questions with respect to consent, which will likely be Google’s principal affirmative defense, are likely to overwhelm any common issues. Therefore, the Court cannot conclude that Plaintiffs have met their burden of demonstrating that the proposed Classes satisfy the predominance requirement.

This Court’s conclusion that Plaintiffs fail to demonstrate predominance is consonant with *Murray v. Fin. Visions, Inc.*, No. 07-2578, 2008 WL 4850328 (D. Ariz. Nov. 7, 2008). *Murray* concerned a Wiretap Act claim brought by a putative class of employees, who sold securities and other investment products, against their employer, a broker-dealer and investment advisor. *Id.* at *1. The employees had contracted with a website hosting service approved by the employer for website and email services. *Id.* The employer asked the website hosting service to intercept and automatically transmit all email sent from or received by any employees to the employer. *Id.* The *Murray* court denied class certification, finding that individual issues predominate with respect to consent. *Id.* at *4. The court held that “[t]he question of consent, either express or implied, is often a fact-intensive inquiry and may vary with the circumstances of the parties.” *Id.*

The individualized nature of the consent inquiry in the instant case is even clearer than that in *Murray*. In *Murray*, the sole source of disclosures, whether from the employer or from other sources, was the SEC regulation and the *Murray* court found that there would be individualized inquiries regarding the impact of that regulation on employees’ knowledge and conduct. In
contrast, here, there are many more disclosures, from Google itself and from the news media, which were unlikely to be uniformly viewed by members of the putative Classes. Accordingly, the Court finds that individualized issues of consent would overwhelm any individual questions.

IV. CONCLUSION

For the foregoing reasons, the Court DENIES Plaintiffs’ Motion for Class Certification. In one sentence on the last page of Plaintiffs’ Reply brief, Plaintiffs request to refile their Motion for Class Certification if this Court were to deny the instant Motion so that Plaintiffs may seek certification of a Rule 23(b)(2) class seeking injunctive relief. See Reply at 20, n.52. The Court rejects Plaintiffs’ request. Plaintiffs have briefed Class Certification three times, and class discovery closed in Dunbar on October 25, 2011. Dunbar II, ECF No. 226, at 3. To the extent that Plaintiffs intended to seek class certification under any theory, Plaintiffs should have done so in the instant Motion. Moreover, Plaintiffs could have requested an opportunity to refile in their Motion, but only sought such relief at the end of their Reply. See United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006) (noting that the Court need not consider arguments raised for the first time in the Reply). Entertaining Plaintiffs’ belated request would prejudice Google, which has been opposing class certification motions in this litigation since September 2011, and which did not have the opportunity in the briefing on the instant Motion to oppose Plaintiffs’ request to refile. Moreover, the Court finds that when asked about Plaintiffs’ request to refile at the hearing, Plaintiffs’ counsel did not provide any persuasive basis for allowing such refiling. Tr. 61:15-63:18. Accordingly, the denial of the Class Certification Motion is with prejudice.

IT IS SO ORDERED.

Dated: March 18, 2014

LUCY H. KOH
United States District Judge
United States District Court
Northern District of California
San Jose Division

Jane Doe 1 and Jane Doe 2,

v.

SuccessfulMatch.com, a California Corporation,

Defendant.

Case No.: 13-CV-03376-LHK

ORDER GRANTING DEFENDANT’S MOTION TO DISMISS PLAINTIFF’S COMPLAINT WITHOUT PREJUDICE AND DENYING DEFENDANT’S MOTION TO STRIKE

Before the Court is Defendant Successfulmatch.com’s (“Defendant”) Motion to Dismiss Plaintiffs’ Complaint or, in the Alternative, to Strike Class Allegations. ECF No. 16 (“Mot.”). Plaintiffs Jane Doe 1 and Jane Doe 2 (collectively “Plaintiffs”) oppose the motion, ECF No. 20 (“Opp.”), and Defendant has filed a Reply, ECF No. 21 (“Reply”). Pursuant to Civil Local Rule 7-1(b), the Court finds this matter appropriate for resolution without oral argument and hereby VACATES the hearing regarding this motion scheduled for April 17, 2014, at 1:30 p.m. The Case Management Conference scheduled for April 17, 2014, at 1:30 p.m. remains as set. Having considered the submissions of the parties, the relevant law, and the record in this case, the Court GRANTS Defendant’s Motion to Dismiss without prejudice, and DENIES Defendant’s Motion to Strike.

Case No.: 13-CV-03376-LHK
ORDER GRANTING DEFENDANT’S MOTION TO DISMISS PLAINTIFFS’ COMPLAINT AND DENYING DEFENDANT’S MOTION TO STRIKE
I. BACKGROUND

A. Plaintiffs’ Factual Allegations

Plaintiff Jane Doe 1, a Canadian resident, and Plaintiff Jane Doe 2, a Washington resident, filed a putative class action complaint on July 19, 2013 against Defendant Successfulmatch.com, a California corporation that operates a variety of dating sites. ECF No. 1 ("Compl.") ¶¶ 1, 4-6. Among the dating sites Defendant operates is PositiveSingles.com, which is marketed to persons with sexually transmitted diseases ("STDs"). Compl. ¶ 1. PositiveSingles.com is designed to help people with STDs meet others who are similarly situated or accepting of members’ medical conditions. Id.

PositiveSingles.com allows members to register and create a profile on the site for free. Id. ¶ 12. If a member decides to use only a free membership, their profile is anonymous. Id. ¶ 15. However, PositiveSingles.com also offers paid memberships, and paid subscribers can disclose more information on their profiles and add a picture. Id. PositiveSingles.com’s home page asks, “Do you wish there was a place where you didn’t have to worry about being rejected or discriminated? This is a warm-hearted and exclusive community for singles and friends with STDs.” Id. ¶ 11. The home page contains a button with the phrase “Join for Free” and a link that states “Totally Free to Place a Fully Anonymous Profile.” Both the button and the link take a potential member to the PositiveSingles.com registration page. Id. ¶ 12.

The registration page states that PositiveSingles.com is a “100% Confidential and Comfortable Community,” and that “[i]t’s absolutely FREE to try out PositiveSingles.com. . . . We do not disclose, sell, or rent any personally identifiable information to any third party organizations.” Id. ¶¶ 13-14. The registration page asks members to provide their first name, email address, age, ethnicity, height, gender, gender of desired partner, location, and their medical condition. ECF No. 17 ("RJN"), Ex. 1B. At the bottom of the registration page, there is a button that states “Continue and Have Fun,” which creates the profile. RJN Ex. 1B. Just above the “Continue and Have Fun” button is a checkbox that states “I am 18+ and have read and agree to the Service Agreement and Privacy Policy,” which links to the Service Agreement (titled “Terms &
Conditions of Service”) and Privacy Policy. RJN Ex. 1A, 1B; Comp. ¶ 16. The Terms &
Conditions of Service state: “To expand the availability of profiles on SuccessfulMatch sites,
profiles may be shared with other sites within the SuccessfulMatch network. By posting or
maintaining a profile on this or any other SuccessfulMatch Network site, you agree and consent
that said profile shall be subject to placement on other SuccessfulMatch Network sites, at the
discretion of SuccessfulMatch, without further notice.” RJN Ex. 1A.3 (emphasis added).

In addition to operating its own dating websites, Defendant allows its customers (called
“affiliate partners”) to create new online dating websites for niche audiences. Specifically, these
affiliate partners contract with the Defendant, and Defendant provides affiliate partners with a
domain name, a site, and Defendant’s central membership database. Compl. ¶¶ 17, 19. Defendant’s
network of affiliated sites serve a diverse set of communities and have domain names such as
Blackpoz.com, HivAidsDating.com, HIVGayMen.com, AllLifestyle4BBW.com, and
ChristianSafeHaven.com, among others. Id. ¶ 2. Because Defendant managed a single database of
member information for all of its sites, a member who registered with an affiliate site could view
the profile information of a PositiveSingles.com member. Id. Therefore, the profile of that member
who registered for PositiveSingles.com could be viewed by members of not only
PositiveSingles.com, but also by members of the various affiliated sites. Id.; Compl. Exs. A-C.

Plaintiffs’ critical allegation is that Defendant fraudulently and deceptively failed to
disclose that profiles created through PositiveSingles.com could be viewed on Defendant’s affiliate
dating sites. Plaintiffs allege that to users, PositiveSingles.com appears to be a stand-alone website.
Compl. ¶ 22. Plaintiffs contend that Defendants induced consumers to sign up for their dating
service by misrepresenting the privacy of their information with statements such as “100%
Confidential and Comfortable Community” and “[Defendant does] not disclose, sell or rent any
personally identifiable information to any third party organizations.” Compl. ¶¶ 13-14. Plaintiffs
further assert that even if members were generally aware of the existence of Defendant’s affiliate
sites, it is not possible for a member to determine exactly how many and what type of sites are
B. Procedural History

Plaintiffs filed their Complaint on July 19, 2013. ECF No. 1. In their Complaint, Plaintiffs allege two causes of action. Plaintiffs allege that Defendant has violated multiple provisions of the Consumer Legal Remedies Act (“CLRA”), Cal. Civ. Code §§ 1750 et seq. Compl. ¶¶ 41-52. Plaintiffs also allege that Defendant has violated the Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200 et seq., which is predicated in part upon the violations of the CLRA. Id. ¶¶ 32-40. Plaintiffs seek to bring this putative class action on behalf of the following proposed class:

All persons who registered for use of the PositiveSingles.com website or any other website indicating that it was “Powered  by PositiveSingles.com” during the four year period prior to the filing date of this Complaint, excluding residents of California.

Id. ¶ 26. The instant case follows a similar suit brought against Defendant in Santa Clara County Superior Court, John Doe v. PositiveSingles.com et al., 111-CV-211208. See RJN. The plaintiff in that case brought claims on behalf of a class of California residents who registered with PositiveSingles.com or any of Defendant’s affiliate sites. Id. at 7. Here, in contrast, Plaintiffs seek redress for non-California users of Defendant’s services.

On December 2, 2013, Defendants filed the instant Motion to Dismiss, as well as a Request for Judicial Notice to include filings from John Doe v. PositiveSingles.com et al. See Mot; RJN. While a district court generally may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion, a court may take judicial notice of documents referenced in the complaint, as well as matters in the public record, without converting a motion to dismiss into one for summary judgment. See Lee v. City of L.A., 250 F.3d 668, 688–89 (9th Cir. 2001). A matter may be judicially noticed if it is either “generally known within the territorial jurisdiction of the trial court” or “can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.” Fed. R. Evid. 201(b). Proper subjects of judicial notice when ruling on a motion to dismiss include pleadings in other relevant proceedings. See Bias v. Moynihan, 508 F.3d 1212, 1225 (9th Cir. 2007). Defendant requests that the Court take judicial notice of the complaint and supporting exhibits filed in John Doe v. PositiveSingles.com, a proceeding in Santa Clara County Superior Court alleging identical UCL and CLRA violations against Defendant on behalf of a different class. RJN at 2. Plaintiff does not oppose Defendant’s request and introduces several orders issued in John Doe in support of its Opposition. Opp. at 1-2. In accordance with the principles discussed above, the Court GRANTS Defendant’s Request for Judicial Notice. The Court also takes judicial notice of the Orders in John Doe that Plaintiffs have provided. See ECF No. 20-1.
Plaintiffs filed their Opposition on December 16, 2013, see Opp., and Defendants filed a Reply on December 23, 2013, see Reply.

II. LEGAL STANDARD

A. Rule 12(b)(6)

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss an action for failure to allege “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (internal citations omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the non-moving party.” Manzarek v. St. Paul Fire & Marine Ins. Co., 519 F.3d 1025, 1031 (9th Cir. 2008).

However, a court need not accept as true allegations contradicted by judicially noticeable facts, Shwarz v. United States, 234 F.3d 428, 435 (9th Cir. 2000), and a “court may look beyond the plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6) motion into a motion for summary judgment, Shaw v. Hahn, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). A court is also not required to “assume the truth of legal conclusions merely because they are cast in the form of factual allegations.” Fayer v. Vaughn, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting W. Min. Council v. Watt, 643 F.2d 618, 624 (9th Cir. 1981)). Mere “conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss.” Adams v. Johnson, 355 F.3d 1179, 1183 (9th Cir. 2004); accord Iqbal, 556 U.S. at 678. Furthermore, “a plaintiff may plead herself out of court” if she “plead[s] facts which establish that [s]he cannot prevail on h[er] . . . claim.” Weisbuch v. Cnty. of L.A., 119 F.3d 778, 783 n.1 (9th Cir. 1997) (internal quotation marks and citation omitted).
B. Rule 9(b)

Claims sounding in fraud or mistake are subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b), which requires that a plaintiff alleging fraud “must state with particularity the circumstances constituting fraud.” Fed. R. Civ. P. 9(b); see Kearns v. Ford Motor Co., 567 F.3d 1120, 1124 (9th Cir. 2009). To satisfy the heightened standard under Rule 9(b), the allegations must be “specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong.” Semegen v. Weidner, 780 F.2d 727, 731 (9th Cir. 1985); Cooper v. Pickett, 137 F.3d 616, 627 (9th Cir. 1997) (allegations of fraud must include “the who, what, when, where, and how” of the misconduct charged). Thus, claims sounding in fraud must allege “an account of the ‘time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations.’” Swartz v. KPMG LLP, 476 F.3d 756, 764 (9th Cir. 2007) (per curiam) (internal quotation marks omitted). The plaintiff must set forth “what is false or misleading about a statement, and why it is false.” In re Glenfed, Inc. Sec. Litig., 42 F.3d 1541, 1548 (9th Cir. 1994) (en banc), superseded by statute on other grounds as stated in Ronconi v. Larkin, 253 F.3d 423, 429 n.6 (9th Cir. 2001).

C. Rule 12(f)

Federal Rule of Civil Procedure 12(f) permits a court to “strike from a pleading an insufficient defense or any redundant, immaterial, impertinent, or scandalous matter.” Fed. R. Civ. P. 12(f). “[T]he function of a 12(f) motion to strike is to avoid the expenditure of time and money that must arise from litigating spurious issues by dispensing with those issues prior to trial.” Sidney-Vinstein v. A.H. Robins Co., 697 F.2d 880, 885 (9th Cir. 1983). Motions to strike are generally disfavored and “should not be granted unless the matter to be stricken clearly could have no possible bearing on the subject of the litigation . . . . If there is any doubt whether the portion to be stricken might bear on an issue in the litigation, the court should deny the motion.” Platte Anchor Bolt, Inc. v. IHI, Inc., 352 F. Supp. 2d 1048, 1057 (N.D. Cal. 2004) (citations omitted). “With a motion to strike, just as with a motion to dismiss, the court should view the pleading in the light most favorable to the nonmoving party.” Id. “Ultimately, whether to grant a motion to strike

D. Leave to Amend

If the Court determines that the complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend “shall be freely given when justice so requires,” bearing in mind “the underlying purpose of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or technicalities.” Lopez v. Smith, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation marks and citation omitted). Nonetheless, a court “may exercise its discretion to deny leave to amend due to ‘undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . ., [and] futility of amendment.’” Carvalho v. Equifax Info. Servs., LLC, 629 F.3d 876, 892-93 (9th Cir. 2010) (quoting Foman v. Davis, 371 U.S. 178, 182 (1962)) (alterations in original).

III. MOTION TO DISMISS

Defendant seeks to dismiss Plaintiffs’ Complaint on a number of grounds, including failure to allege reliance or harm as required by the UCL and CLRA; failure to allege a claim under any specific prong of the UCL; lack of duty to disclose; and lack of actionable misrepresentation or omission. Mot. at 4-16; Reply at 1-2. For the reasons stated below, the Court finds that Plaintiffs have failed to allege reliance and injury in fact for their UCL and CLRA claims. Because reliance and injury are essential elements of both of Plaintiffs’ causes of action, the Court grants the Motion to Dismiss in full and declines to address Defendant’s remaining bases for dismissal. The Court begins by discussing the legal standard for reliance and injury under the UCL and CLRA and then applies those standards to the allegations in the Complaint.

A. Legal Standard

The UCL broadly prohibits “any unlawful, unfair or fraudulent business act or practice.” Cal. Bus. & Prof. Code § 17200. The CLRA prohibits a host of unfair and deceptive practices,
including various forms of misrepresentation. See Cal. Civil Code § 1770. Both the UCL and the
CLRA prohibit not only affirmative misrepresentations, but also material omissions that deceive
reasonable consumers. In the instant case, Plaintiffs contend that Defendant has violated the unfair
and fraudulent prong of the UCL through both affirmative misrepresentations regarding the privacy
of users’ profiles on PositiveSingles.com and through the omission of material facts regarding the
sharing of information across the various SuccessfulMatch affiliate websites. In addition, Plaintiffs
contend that through these same misrepresentations and omissions, Defendant has violated the
CLRA. Plaintiffs finally contend that Defendant has violated the unlawful prong of the UCL,
which incorporates violations of other statutes, because Defendant has violated the CLRA.

Both the CLRA and the UCL require Plaintiffs to demonstrate standing. A plaintiff may
bring a claim under the CLRA so long as she “suffer[ed] any damage as a result of” a proscribed
practice under the CLRA. Cal. Civ. Code § 1780(a). This means that to adequately plead a CLRA
claim, a plaintiff must allege that she relied on the defendant’s alleged misrepresentation and that
she suffered economic injury as a result. Durell v. Sharp Healthcare, 183 Cal. App. 4th 1350, 1367
(2010).

Likewise, to establish standing under the UCL, a plaintiff must demonstrate that she
“suffered injury in fact and [ ] lost money or property as a result of the unfair competition.” Cal.
Bus. & Prof. Code § 17204.³ Interpreting this statutory language, California courts have held that
when the “unfair competition” underlying a plaintiff’s UCL claim consists of a defendant’s
misrepresentation, a plaintiff must have actually relied on the misrepresentation, and suffered
economic injury as a result of that reliance, to have standing to sue. See In re Tobacco II Cases, 46
Cal. 4th 298, 326 (2009). California courts have subsequently extended the actual reliance
requirement to claims brought under the UCL’s unlawful prong to the extent “the predicate
unlawful conduct is based on misrepresentations.” Durell, 183 Cal. App. 4th at 1355; accord
Kwikset Corp. v. Superior Court, 51 Cal. 4th 310, 326 (2011). Moreover, in Kwikset Corp. v.

3 A plaintiff who has standing under the UCL’s “lost money or property” requirement will have
suffered the requisite “damage” for purposes of establishing CLRA standing. Hinojos v. Kohl’s
Corp., 718 F.3d 1098, 1108 (9th Cir. 2013).
Superior Court, the California Supreme Court suggested that the actual reliance requirement applies whenever the underlying misconduct in a UCL action is fraudulent conduct. See 51 Cal.4th 310, 326 (2011). In line with this authority, this Court has concluded “that the actual reliance requirement also applies to claims under the UCL’s unfair prong to the extent such claims are based on fraudulent conduct.” See Kane v. Chobani, Inc., No. 12-2425, 2013 WL 5289253, at *6 (N.D. Cal. Sept. 19, 2013). Accordingly, this Court has consistently required allegations of actual reliance and injury at the pleading stage for claims under all three prongs of the UCL where such claims are premised on misrepresentations. See Kane v. Chobani, Inc., No. 12-2425, 2014 WL 657300, at *5 (N.D. Cal. Feb. 20, 2014).

This showing of actual reliance under the UCL requires a plaintiff to allege that “the defendant’s misrepresentation or nondisclosure was an immediate cause of the plaintiff’s injury-producing conduct.” Tobacco II, 46 Cal. 4th at 326 (internal quotation marks omitted). “A plaintiff may establish that the defendant’s misrepresentation is an immediate cause of the plaintiff’s conduct by showing that in its absence the plaintiff in all reasonable probability would not have engaged in the injury-producing conduct.” Id. (internal quotation marks omitted). While a plaintiff need not demonstrate that the defendant’s misrepresentations were “the sole or even the predominant or decisive factor influencing his conduct,” the misrepresentations must have “played a substantial part” in the plaintiff’s decision-making. Id.

For a plaintiff to bring UCL and CLRA claims on the basis of omissions, the omission must either be “contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose.” Donohue v. Apple, Inc., 871 F. Supp. 2d 913, 925 (N.D. Cal. 2012) (quoting Baltazar v. Apple, Inc., 10-3231, 2011 WL 588209, at *4 (N.D. Cal. Feb. 10, 2011)). The California Court of Appeal has held that there are four circumstances in which a failure to disclose a fact can constitute fraud or deceit:

(1) when the defendant is the plaintiff’s fiduciary; (2) when the defendant has exclusive knowledge of material facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations that are misleading because some other material fact has not been disclosed.
Collins v. eMachines, Inc., 202 Cal. App. 4th 249, 255 (2011). To establish the causal nexus between the omission and a plaintiff’s harm, a plaintiff must plead that she would not have purchased the product or service at issue if she had known the material fact that Defendant allegedly omitted. See Kwikset, 51 Cal. 4th at 327; Donohue, 871 F. Supp. 2d at 920.

Here, the gravamen of Plaintiffs’ claims under the UCL and CLRA is that Defendants fraudulently misrepresented the confidentiality of member information by omitting the fact that members’ profiles are replicated on Defendants’ network of affiliate sites. Compl. ¶¶ 20-22. This omission induced individuals with STDs—who have a strong interest in keeping their medical information private—to sign up for Defendant’s dating service. Id. ¶¶ 1, 11. To demonstrate standing under the UCL and CLRA under this theory, Plaintiffs must allege that they actually relied on Defendant’s misrepresentations and suffered economic injury as a result of that reliance.

B. Reliance

Defendant argues that Plaintiffs have not alleged that they viewed or relied on any of the alleged misrepresentations on the PositiveSingles.com website. Mot. at 10, 15. The Court agrees for the reasons stated below.

The Complaint and supporting exhibits describe different representations made on the PositiveSingles.com homepage and registration page, such as “100% Confidential and Comfortable Community,” “This is a warm-hearted and exclusive community for singles and friends with STDs,” “We care about your privacy more than other sites,” and “We do not disclose, sell or rent any personally identifiable information to any third party organizations.” Id. ¶¶ 11-13; RJN Ex. B. The registration page also requires clicking a box that states “I am 18+ and I have read and agree to the Service Agreement and Privacy Policy.” RJN Ex. B.

The Complaint lacks allegations of what, if any, purported misrepresentations the two named Plaintiffs, Jane Doe 1 and Jane Doe 2, actually read. Plaintiffs have failed to specifically allege that they saw any of the statements that they claim are misleading, or how the website statements impacted their decisions to register with Defendant’s website. Plaintiffs’ generalized allegations that Defendants “preyed on the vulnerability of the members of the public that tested...
positive for STDs” and that Defendants “lured [members] in with empathetic sounding statements” are insufficient to meet the pleading requirement. Rather, Plaintiffs must, at a minimum, allege that they actually viewed the representations that they now contend are misleading. Furthermore, Plaintiffs have not pleaded any facts to meet the “but for” test for fraudulent omissions, as they have failed to allege how knowledge of Defendant’s omissions about affiliated sites would have impacted Plaintiffs’ decision to register for PositiveSingles.com. See Donohue, 871 F. Supp. 2d at 920.

Beyond pointing to general statements about Defendant’s conduct, Plaintiffs rely on In re Steroid Hormone Prods. Cases, 181 Cal. App. 4th 145 (2010), and McAdams v. Mornier, Inc., 182 Cal. App. 4th 174 (2010), for the proposition that in cases involving omissions, an allegation that the omission is material is sufficient without any independent allegation of reliance. Opp. at 9-10. Plaintiffs’ citation to these cases is unavailing. These cases address the actual reliance requirements of unnamed class members, not named plaintiffs, in UCL class actions premised on fraudulent misrepresentations. Steroid Hormone, 181 Cal. App. 4th at 157; McAdams, 182 Cal. App. 4th at 182. Neither case purports to excuse named plaintiffs from the pleading requirements necessary to establish standing under the UCL and CLRA. See Steroid Hormone, 181 Cal. App. 4th at 154 (“While a named plaintiff in a UCL class action now must show that he or she suffered injury in fact and lost money or property as a result of the unfair competition, once the named plaintiff meets that burden, no further individualized proof of injury or causation is required to impose restitution liability against the defendant in favor of absent class members.”); McAdams, 182 Cal. App. 4th at 189 (“[O]nly the representative plaintiff need meet the [standing] requirement.”). In fact, Steroid Hormone makes clear that the named plaintiff pleaded the “but for” allegations necessary in omissions cases.4 181 Cal. App. 4th at 150 (“[Plaintiff states he] would not have purchased those products had he known they were illegal to possess without a prescription.”). The Complaint in the instant case lacks similar allegations that the named Plaintiffs would not have purchased a product

4 McAdams remanded the case to the trial court for a determination of the named plaintiff’s standing under the UCL, and thus does not discuss standing allegations explicitly. 182 Cal. App. 4th at 192.
or service if the omissions had been disclosed.

Accordingly, the Court is not persuaded that Plaintiffs have pleaded the facts necessary to allege reliance on Defendant’s alleged misrepresentations and omissions and GRANTS Defendant’s Motion to Dismiss on this basis. Because this appears to be a pleading deficiency and not due to implausibility of the facts alleged, the Court grants Plaintiffs leave to amend the Complaint to cure this deficiency.

C. Economic Injury

Defendant also contends that it is unclear from the Complaint whether Plaintiffs suffered any injury and that Plaintiffs have not alleged that they were actually members of PositiveSingles.com or that they paid for subscriptions. Mot at 3 n.1, 15. For the reasons stated below, the Court agrees with Defendant.

The Complaint states that initial registration with PositiveSingles.com is free and anonymous, consistent with Defendant’s representations on its website. See Compl. ¶¶ 12, 15; RJN Ex. 1B. Members who elect to purchase paid subscriptions can post pictures on their profile and disclose more information than members who do not pay for a membership. Compl. ¶ 15. The Complaint’s accompanying exhibits are screenshots of one of Plaintiff’s profiles on different affiliate sites, such as Blackpoz.com, HivAidsDating.com, and HIVGayMen.com, and the profiles all include a picture, suggesting that at least one of the named Plaintiffs had a paid membership. Exs. A-C. The picture appears to be the same in each profile, and each profile indicates the member’s “status” as “Recommended/Gold Member . . . PositiveSingles.com/ SuccessfulMatch.” See id.

Interpreted in a light most generous to the Plaintiffs, the Complaint and accompanying exhibits support the inference that either Jane Doe 1 or Jane Doe 2 was a paid member of PositiveSingles.com. However, Plaintiffs do not specify whose profile is shown in the Complaint exhibits, nor does the Complaint specify whether the other named Plaintiff signed up for PositiveSingles.com. Moreover, the Complaint does not even make clear that either Plaintiff registered with PositiveSingles.com directly. Rather, it is equally possible that the Plaintiff whose
Because the crux of Plaintiffs’ theory of harm stems from misrepresentations and omissions made on PositiveSingles.com home page and registration page, it follows that Plaintiffs should identify with particularity on which of Defendants’ sites Plaintiffs registered. See Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (“Averments of fraud must be accompanied by ‘the who, what, when, where, and how’ of the misconduct charged.”). Plaintiffs have not done so here.

Most importantly, Plaintiffs also fail to make clear that they suffered any economic injury as a result of Defendant’s conduct. Plaintiffs again point to generalized statements to address this pleading deficiency, but conclusory allegations such as “Plaintiffs and the Class have suffered injury in the form of actionable losses of money,” without anything explicit about how those losses were sustained, is insufficient to satisfy the pleading requirements.

Accordingly, the Court GRANTS Defendant’s Motion to Dismiss Plaintiffs’ Complaint for failure to allege with particularly the economic injury sustained as a result of Defendant’s conduct. Again, the problem appears to be more a pleading deficiency than a lack of plausibility. Because this deficiency could be cured by clearer factual allegations regarding how Plaintiffs suffered economic damages, the Court grants Plaintiffs leave to amend.

IV. MOTION TO STRIKE

Defendant moves to strike Plaintiff’s nationwide class allegations. Mot. at 16-18; Reply at 3. Specifically, Defendant asserts that Plaintiffs’ claims on behalf of the nationwide class must be stricken because California’s choice-of-laws analysis, articulated in Mazza v. American Honda Motor Co., 666 F.3d 581 (9th Cir. 2012), prohibits the application of California’s consumer protection laws to non-California plaintiffs in this case. See Mot. at 16-17. Plaintiffs respond by noting that Defendant’s Terms of Service require the application of California law in governing disputes between PositiveSingles.com members and Defendant. Opp. at 15. Plaintiffs also argue that a choice-of-law analysis must be made on a developed factual record, and not on a motion to dismiss. Id. at 16. For the reasons stated below, the Court agrees with Plaintiffs as to the latter

5 It is not clear that the named Plaintiff whose profile pages are not attached to the Complaint registered for any Defendant website or affiliated website.
point, and need not make a determination as to the applicability of Defendant’s choice-of-law
provision at this stage.

In Mazza, a putative class of plaintiffs sued Honda for violations of the UCL, California’s
False Advertising Law (“FAL”), and CLRA in connection with Honda’s marketing of its
"Collision Mitigation Braking System." 666 F.3d at 586-87. The Ninth Circuit reversed the district
court’s certification of a nationwide class after concluding that, “[u]nder the facts and
circumstances of this case,” California’s choice-of-law rules dictated that “each class member’s
consumer protection claim should be governed by the consumer protection laws of the jurisdiction
in which the transaction took place.” Id. at 594.

Here, the Court finds that striking the nationwide class allegations at this stage of the case
would be premature. The Ninth Circuit’s opinion in Mazza—which was decided at the class
certification stage and not on a motion to dismiss—depended heavily on a detailed choice-of-law
analysis that compared how various states’ consumer protection laws applied to the facts of the
plaintiffs’ claims. See id. at 589-94. By contrast, the briefing at the instant stage of litigation lacks
the detail necessary to conduct this analysis. Defendant—who bears the burden of demonstrating
“that foreign law, rather than California law, should apply to class claims” in a California choice-of-law
analysis, Washington Mutual Bank, FA v. Superior Court, 24 Cal. 4th 906, 921 (2001)—
provides no support for Defendant’s position that foreign law conflicts with California law, let
alone that this conflict is so severe as to preclude applying California law to Plaintiffs’ class
claims. Absent the sort of detailed choice-of-law analysis that guided the Ninth Circuit in Mazza,
the Court declines to evaluate how California’s choice-of-law rules affect Plaintiffs’ class claims at
this time. This conclusion is in accord with this Court’s decision in Brazil v. Dole Food Co., No.
12-1831, 2013 WL 5312418, at *11 (N.D. Cal. Sept. 23, 2013), as well as the decisions of
numerous other courts within the Ninth Circuit, which have declined, even after Mazza, to conduct
the choice-of-law analysis at the pleading stage, see Werdebaugh v. Blue Diamond Growers, No.
Accordingly, the Court DENIES Defendant’s Motion to Strike Plaintiffs’ nationwide class claims.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS with leave to amend Defendant’s Motion to Dismiss, on the basis that Plaintiffs failed to plead the reliance and injury necessary to state a claim. The Court DENIES Defendant’s Motion to Strike Plaintiff’s Class Allegations. If Plaintiffs wish to file an amended complaint addressing the deficiencies identified in this Order, Plaintiffs must do so within 21 days of this Order. Plaintiffs may not add new claims or parties without seeking Defendant’s consent or leave of the Court pursuant to Federal Rule of Civil Procedure 15. Plaintiffs’ failure to file an amended complaint within 21 days of this Order or failure to cure the deficiencies in this Order will result in a dismissal of this case with prejudice.

IT IS SO ORDERED.

Dated: April 16, 2014

LUCY H. KOh
United States District Judge
UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

CIVIL ACTION NO. 3:12-CV-00396 (VLB)

In re Trilegiant Corporation, Inc.

March 28, 2014

MEMORANDUM OF DECISION GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED AMENDED CLASS ACTION COMPLAINT OR, IN THE ALTERNATIVE, TO STRIKE PORTIONS OF THE COMPLAINT [DKT. 189]

I. Introduction

The Plaintiffs, Debra Miller ("Miller"), Brittany DiCarolis ("DiCarolis"), Hope Kelm ("Kelm"), Jennie H. Pham ("Pham"), Brett Reilly ("Reilly"), Juan M. Restrepo ("Restrepo"), Brian Schnabel, Edward Schnabel, Lucy Schnabel, Annette Sumlin ("Sumlin"), Regina Warfel ("Warfel"), and Debbie Williams ("Williams"), bring this proposed class action against three groups of Defendants, the Trilegiant Defendants, which includes Affinion Group, LLC ("Affinion"), Trilegiant Corporation, Inc. ("Trilegiant"), and Apollo Global Management, LLC ("Apollo"), the Credit Card Defendants, which includes Bank of America, N.A. ("Bank of America"), Capital One Financial Corporation ("Capital One"), Chase Bank USA, N.A. ("Chase"), Citibank, N.A. ("Citibank"), Citigroup, Inc. ("Citigroup"), Chase Paymentech Solutions, LLC ("Paymentech"), and Wells Fargo Bank, N.A. ("Wells Fargo"), and the E-Merchant Defendants, which includes 1-800-Flowers.com, Inc. ("1-800 Flowers"), Beckett Media LLC ("Beckett"), Buy.com, Inc. ("Buy.com"),
Classmates International, Inc. ("Classmates"), Days Inns WorldWide, Inc. ("Days Inns"), Wyndham WorldWide Corporation ("Wyndham"), FTD Group, Inc. ("FTD"), Hotwire, Inc. ("Hotwire"), IAC/InterActiveCorp ("IAC"), Shoebuy.com, Inc. ("Shoebuy"), PeopleFindersPro, Inc. ("PeopleFinder"), Priceline.com, Inc. ("Priceline"), and United Online, Inc. ("United Online").

Before the Court is the Defendants’ Consolidated Motion to Dismiss or, in the Alternative, to Strike Various Portions of the Complaint. [Dkt. 189]. Several of the Defendants have also filed separate motions to dismiss, strike, or stay the proceedings on various other grounds. Those motions will be decided in other subsequent orders. For the reasons that follow, Defendants’ motion to dismiss or in the alternative to strike is GRANTED in part and DENIED in part as set forth herein.

II. Factual Background

The following facts and allegations are taken from the Plaintiffs’ Consolidated Amended Class Action Complaint (the “Complaint”). [Dkt. 141, hereinafter “CAC at ¶”]. The Plaintiffs allege that through the Defendants’ deceptive, unfair, and fraudulent business practices, the Plaintiffs were enrolled in Trilegiant membership programs without their knowledge or explicit consent and that their program memberships remained extant for months and in some cases years. CAC at ¶ 1. The alleged scheme was initiated and orchestrated by Trilegiant with the help of its parent companies, Apollo and Affinion, but was only successful because of a series of quid pro quo agreements executed with several of the E-Merchant Defendants and the willing participation of the Credit Card Defendants. CAC at ¶ 3.

The Complaint asserts that Trilegiant sold memberships in its discount membership clubs, which the Plaintiffs conclude have “no real value.” CAC at ¶ 4. Trilegiant marketed its memberships in collaboration with and to the
customers of various E-Merchant Defendants. CAC at ¶ 72. The E-Merchant Defendants received signing bonuses and/or substantial “bounties,” equal to a percentage of “every dollar” Trilegiant earned from the E-Merchant customers that purchased Trilegiant products and services. CAC at ¶¶ 6, 7. The Plaintiffs also allege that several of the Credit Card Defendants formed partnerships with Trilegiant to allow Trilegiant to advertise and sell “credit guard type” programs to their customers, and others had marketing contracts requiring the Credit Card Defendants to send Trilegiant’s hard copy mail advertisements to its customers with the customer’s credit card or bank account statements. CAC at ¶¶ 11(b), 49. The Complaint does not allege, and the Court does not construe it to allege, that the Credit Card Defendants are included as E-Merchants.

The Plaintiffs further allege that the written agreements with the E-Merchant Defendants detailed at least four of the insidious business practices that were used to further the scheme’s illegitimate ends.¹ CAC at ¶ 7. First, the Plaintiffs allege that Trilegiant and the E-Merchant Defendants engaged in post-transaction marketing by creating “a false and deceptive appearance,” implying “that [Trilegiant’s] offers for discount Membership Programs [were] part of the consumers’ original transactions with the e-merchants.” CAC at ¶ 74. The Plaintiffs also allege that the E-Merchant Defendants had review authority over these designs and have final approval of any advertisement language. CAC at ¶ 117. To induce the feeling that the membership offer was from the E-Merchant Defendant, and not Trilegiant, the Plaintiffs allege that Defendants used three

¹ The Plaintiffs do not make similar allegations for the agreements between Trilegiant and the Credit Card Defendants.
different design tactics: (1) “‘interstitial’ sales offer pages” for Trilegiant’s products, which appear between the checkout page and the confirmation page for the customer’s primary, e-merchant purchase; (2) “‘pop up’ windows, detailing the offers, which appear on top of the e-merchant’s confirmation page; and (3) a hyperlink to an enrollment offer (or ‘banners’) that are included on the [E]-[M]erchant Defendant’s confirmation page.” CAC at ¶ 74. Importantly, all of these marketing tactics were used before the customer received confirmation of its purchase with the E-Merchant Defendant. CAC at ¶¶ 7(a), 117.

Second, the Plaintiffs allege that the E-Merchant Defendants engaged in “datapass” with Trilegiant, meaning that each individual E-Merchant Defendant passed its customers’ confidential billing information to Trilegiant without the customers’ explicit consent or knowledge; according to the Plaintiffs, this process is meant to facilitate further online purchases because the customers are not required to reenter their credit card or debit account information to complete a secondary transaction with Trilegiant. CAC at ¶¶ 7(a), 75-80. While it is unclear from the pleadings how and when this process exactly occurs, the Plaintiffs allege that there is an interface token that stores each customer’s confidential billing information entered while making the primary purchase on the E-Merchant’s website. CAC at ¶ 117(c). When the customer clicks on a link, a banner, or a pop-up window that leads to Trilegiant’s disguised offer page, the token transfers the customer’s confidential billing information directly to Trilegiant, presumably before the customer accepts the offer. Id. The Plaintiffs then allege that after the customers unknowingly agree to purchase Trilegiant’s
product, they are returned to their original purchase and only then receive confirmation of the original E-Merchant transaction. CAC at ¶¶ 7(a), 117(c). The customer is not aware, however, that on the backend, the token has transferred its personal billing information to Trilegiant, which Trilegiant uses to begin automatically charging the customer a monthly membership fee. CAC at ¶ 117. The Plaintiffs conclude that “[b]ecause the consumer never has to enter any credit card information during a transaction with Trilegiant, they reasonably believe that they did not make any additional purchases apart from their original transaction with an E-Merchant Defendant.” CAC at ¶ 80.

Third, Trilegiant practices negative option billing, meaning that consumers are automatically charged a monthly membership fee “unless the consumers take affirmative steps to cancel the membership.” CAC at ¶ 81. The consumers are only made aware of this billing practice by a disclosure in “exceedingly fine print” on Trilegiant’s “offer” page. CAC at ¶ 81. This is the only detail the Plaintiffs provide regarding the content or presentation of Trilegiant’s actual offer page.

Finally, the Plaintiffs allege that months or years after the consumer realizes that he or she has been charged an illegitimate monthly membership fee, the Defendants make it nearly impossible to obtain a full refund through their “refund mitigation strategy.” CAC at ¶ 8. Refund mitigation is explicitly employed to minimize “the amount of improper charges [the Defendants] would have to refund to the millions of confused and angry consumers . . . .” CAC at ¶ 83. As part of this strategy, Trilegiant’s call-center employees utilize several stall tactics to frustrate customers attempts to cancel their memberships and receive
refunds, including “quickly cancel[ing memberships] without a refund as soon as
the customer complains, and demanding that the request for cancelation be in
writing.” CAC at ¶ 8. The Plaintiffs allege that the E-Merchant Defendants are
directly integrated in creating and administering this strategy and have the
opportunity to select how many “rebuttals” the call-center employee may pitch
during a cancelation call, to participate in the calls, and to review the call-center
scripts. CAC at ¶ 8. Disturbingly, the Plaintiffs also allege that before a customer
requesting a refund would reach the rebuttal-step stage, call-center employees
were instructed to “tell the customers that they somehow signed up for the
Membership Programs through their credit card company,” instead of explaining
to them “the real method” of their enrollment. CAC at ¶ 86. As proof of this
intentional deception, the Plaintiffs allege that a 1-800 Flowers representative
complained to a Trilegiant representative that “‘we have had increasingly more
frequent feedback from our own teams that your agents are telling our customers
to call us’” when the customers call Trilegiant to cancel their memberships. CAC
at ¶ 133. Furthermore, the call centers were supposedly only able to give a
maximum refund for two months of membership fees, but if the customer used
words such as “fraud,” “attorney,” “attorney general,” or “lawsuit” while on the
call, they would be transferred to a call-center manager and could then receive a
full refund. CAC at ¶ 86. Ultimately, most customers did not obtain a full refund
by calling Trilegiant and were required to submit a written refund request. CAC at
¶ 87.
Once the customers were enrolled in a Trilegiant membership program, the Plaintiffs allege that the E-Merchant and Trilegiant Defendants could only have executed their scheme with the willing participation of the various Credit Card Defendants because the Credit Card Defendants were ultimately responsible for processing the charges. CAC at ¶¶ 3, 8, 11, 73. The Plaintiffs concluded that the Credit Card Defendants were knowing-participants in the scheme by, either intentionally or recklessly, ignoring their own policies and their own sophisticated anti-fraud software when reviewing and processing the membership charges. CAC at ¶¶ 88-95. As proof for this conclusion, the Plaintiffs generally refer to the “thousands” of complaints that the Credit Card Defendants received over the years the scheme was perpetrated. CAC at ¶¶ 14, 88-103. The Plaintiffs further assert that

[despite [the] abundant evidence that Trilegiant’s business practices did not meet the Defendant Credit Card Companies’ merchant rules, and despite their knowledge that Trilegiant’s membership “club” charges are among the highest sources of complaints brought to the attention of their fraud monitoring groups, the Defendant Credit Card Companies continued to process millions of questionable credit and debit charges every month without first verifying the charges with the account holder, as they do with other questionable credit card charges.

CAC at ¶ 93. The Plaintiffs posit that the only explanation for the Credit Card Defendants’ refusal to stop processing the monthly membership charges, is that the Credit Card Defendants were knowing-participants in and “profited from the . . . fraudulent scheme—a scheme that could not have operated without” their participation. CAC at ¶¶ 85 103. The Plaintiffs do not allege that the Credit Card
Defendants had any written agreement with the Trilegiant or E-Merchant Defendants specifically related to the alleged online marketing scheme at issue in this case. Moreover, the Plaintiffs do not allege that the Credit Card Defendants had actual knowledge of the fraud, just that they possessed constructive knowledge of the scheme given the “thousands” of complaints they received over the years the scheme was being perpetrated and Trilegiant’s alleged infamous reputation for engaging in fraudulent business conduct. CAC at ¶ 103. The Plaintiffs’ only factual allegation related to Trilegiant's purported infamous business reputation relates to the prior class action litigation and the publicity from the prior government settlements and congressional investigation.

The Plaintiffs also allege that to further the fraudulent scheme, the Defendants “repeatedly used interstate wire and mail communications” including sending “thousands” of messages to the other Defendants discussing various aspects of the scheme. CAC at ¶ 160. The Plaintiffs do not allege, however, the actual contents of any such messages aside from the information contained in the credit card and bank account statements that were sent to the Plaintiffs highlighting the membership fee charges. CAC at ¶ 160(h). Furthermore, the Plaintiffs do not allege the details of any one fraudulent statement that was made by any Defendant to the Plaintiffs.

Plaintiff DiCarolis alleges that she was a citizen of Oregon who made a purchase on TigerDirect’s website prior to July 2010 using a Chase credit card; shortly thereafter, the Plaintiff was enrolled in a Trilegiant membership program, but only noticed the recurring charges around January 2012. CAC at ¶ 24.
Plaintiff Kelm alleges that she was a citizen of Texas who made an online purchase on Days Inns’ website in June 2009 using a credit card; shortly thereafter, she was enrolled in a Trilegiant membership program, but only noticed the recurring monthly charges on her credit card statements more than two years later, around November 2011. CAC at ¶ 25.

Plaintiff Pham alleges that she was a citizen of California who made an online purchase on Shoebuy’s website on December 3, 2009 using her Chase credit card; shortly thereafter, she was enrolled in a Trilegiant membership program, but only noticed the recurring monthly credit card charges nearly two years later, around September 2011. CAC at ¶ 26.

Plaintiff Reilly alleges that he was a citizen of California who made an online purchase on Buy.com’s website with his Chase credit card; shortly thereafter, he was enrolled in a Trilegiant membership program, but only noticed the recurring monthly credit card charges approximately two years later, around January 2012. CAC at ¶ 27.

Plaintiff Restrepo alleges that he was a citizen of Arizona and claims that his Chase credit card was charged for a Trilegiant membership program starting on May 9, 2007, but he only noticed the recurring monthly credit card charges nearly four years later in April 2011. CAC at ¶ 28. He does not allege that he made any online purchases from an E-Merchant Defendant. Id.

Plaintiff Brian Schnabel alleges that he was a citizen of California and claims that he was told he enrolled in a Trilegiant membership program through
Priceline. CAC at ¶ 29. The monthly membership fees were charged to his CitiDiamond Preferred credit card beginning on December 20, 2007, but he only noticed the recurring monthly credit card charges more than two years later in March or April 2010. Id.

 Plaintiffs Edward and Lucy Schnabel allege that they were citizens of California and claim that they were told they enrolled in a Trilegiant membership program through a rebate. CAC at ¶ 30. The monthly membership fees were charged to their United Mileage Plus credit card beginning on September 21, 2009, but they only noticed the recurring monthly credit card charges six months later on March 9, 2010. Id.

 Plaintiff Sumlin alleges that she was a citizen of Alabama and claims that her Wells Fargo checking account was charged in April 2012 for a Trilegiant membership. CAC at ¶ 31. She further alleges that her checking account was charged for at least the three or four months prior to April 2012. She does not claim to have been on an E-Merchant Defendant website or that she was charged for her Trilegiant membership by a Credit Card Defendant. Id.

 Plaintiff Timmcke alleges that she was a citizen of New Mexico who made an online purchase through PeopleFinder's website around August 2011 using a debit card; shortly thereafter, she was enrolled in a Trilegiant membership program, but only noticed the recurring debits two months later, around October 2011. CAC at ¶ 32.
Plaintiff Warfel alleges that she was a citizen of Ohio who had a phone call with Chase’s automated services in December 2004; shortly thereafter, her Chase credit card was charged for a Trilegiant membership, but she only noticed the recurring monthly credit card charges more than six years later, around January 2011. CAC at ¶ 33. She does not allege that she was on an E-Merchant website.

Plaintiff Williams alleges that she was a citizen of North Carolina who made an online hotel reservation through Priceline using her Wachovia debit card on or around May 26, 2009; shortly thereafter, she was enrolled in a Trilegiant membership program, but only noticed the recurring charges around October 2011. CAC at ¶ 34.

All of the Plaintiffs allege that they did not know of or consent to purchasing a Trilegiant membership and did not use any Trilegiant memberships’ services. CAC at ¶ 35. Each further alleges that he or she did not receive a full refund. CAC at ¶¶ 24-34. Only Plaintiff DiCarolis, however, alleges that Trilegiant continued to charge her account even after she canceled or attempted to cancel her membership. CAC at ¶ 24.

Based on these allegations, the Plaintiffs have requested individual and class-based relief under several federal and state statutes. The Defendants’ have moved to dismiss the Complaint for failure to state a claim for relief and, in the alternative, to strike portions of the Complaint.
III. Standard of Review

“A pleading that states a claim for relief must contain: . . . (2) a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). “To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” Sarmiento v. United States, 678 F.3d 147, 152 (2d Cir. 2012) (quoting Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)). While Rule 8 does not require detailed factual allegations, “[a] pleading that offers ‘labels and conclusions’ or ‘formulaic recitation of the elements of a cause of action will not do.’ Nor does a complaint suffice if it tenders ‘naked assertion[s]’ devoid of ‘further factual enhancement.’” Iqbal, 556 U.S. at 678 (citations omitted). “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of ‘entitlement to relief.’” Id. (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 557 (2007)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. (citations and internal quotation marks omitted).

In considering a motion to dismiss for failure to state a claim, the Court should follow a “two-pronged approach” to evaluate the sufficiency of the complaint. Hayden v. Paterson, 594 F.3d 150, 161 (2d Cir. 2010). “A court ‘can choose to begin by identifying pleadings that, because they are no more than conclusions, are not entitled to the assumption of truth.’” Id. (quoting Iqbal, 556 U.S. at 679). “At the second step, a court should determine whether the ‘well-
pleaded factual allegations,' assumed to be true, 'plausibly give rise to an entitlement to relief.’” *Id.* (quoting *Iqbal*, 556 U.S. at 679). “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citations and internal quotation marks omitted).

In general, the Court’s review on a motion to dismiss pursuant to Rule 12(b)(6) “is limited to the facts as asserted within the four corners of the complaint, the documents attached to the complaint as exhibits, and any documents incorporated by reference.” *McCarthy v. Dun & Bradstreet Corp.*, 482 F.3d 184, 191 (2d Cir. 2007). The Court may also consider “matters of which judicial notice may be taken” and “documents either in plaintiffs' possession or of which plaintiffs had knowledge and relied on in bringing suit.” *Brass v. Am. Film Techs., Inc.*, 987 F.2d 142, 150 (2d Cir.1993); *Patrowicz v. Transamerica HomeFirst, Inc.*, 359 F. Supp. 2d 140, 144 (D. Conn. 2005).

IV. Discussion

The Court will separately address each of the causes of action that the Defendants’ argue should be dismissed.


The Defendants have moved to dismiss the Plaintiffs’ substantive RICO claims on several grounds: (1) the Plaintiffs failed to sufficiently plead a RICO enterprise; (2) the Plaintiffs failed to sufficiently plead a pattern of racketeering activity; and (3) some of the Plaintiffs’ claims are barred by the relevant statute of
limitations. [Dkt. 189-1, Memorandum of Law in Support of Defendants’ Motion to Dismiss Plaintiffs’ Consolidated Class Action Complaint or, in the Alternative, to Strike Portions of the Complaint, p. 10-25, hereinafter “MTD”]. The Plaintiffs respond by arguing that they have sufficiently pled an enterprise among all of the Defendants, they have sufficiently alleged with appropriate particularity the pattern of racketeering activity, and none of the Plaintiffs’ claims are barred by the statute of limitations. [Dkt. 219, Plaintiffs’ Consolidated Memorandum of Law in Opposition to Defendants’ Motion to Dismiss, p. 5-37, hereinafter “Opp.”]. The Court finds that the Plaintiffs have not sufficiently pled a substantive RICO violation to sustain the Defendants’ motion to dismiss.

Notwithstanding the degree of particularity required by the pleading rules in the Federal Rules of Civil Procedure, “[t]o establish a RICO claim, a plaintiff must show: (1) a violation of the RICO statute . . . ; (2) an injury to business or property; and (3) that the injury was caused by the violation of” the RICO statute. Cruz v. FXDirectDealer, LLC, 720 F.3d 115, 120 (2d Cir. 2013) (citations and internal quotation marks omitted). To prove a violation of the RICO statute, a plaintiff must plead that the violation occurred through the “(1) conduct, (2) of an enterprise, (3) through a pattern (4) of racketeering activity.” Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 496 (1985); see also Lundy v. Catholic Health Sys. of Long Island Inc., 711 F.3d 106, 118 (2d Cir. 2013) (the complaint must also allege “‘injury to business or property as a result of the RICO violation . . . ’ [and] [t]he pattern of racketeering activity must consist of two or more predicate acts of
racketeering”) (quoting Anatian v. Coutts Bank (Switz.) Ltd., 193 F.3d 85, 88 (2d Cir. 1999)).

i. RICO Enterprise

The Defendants argue that the Plaintiffs have not adequately pled a RICO enterprise because the Plaintiffs do not allege one enterprise “with an ascertainable structure that works together for a common purpose.” MTD p. 13. They claim that at best the Plaintiffs’ allegations show that there were several individual agreements between Trilegiant and each individual E-Merchant, demonstrating parallel conduct, not a unified or concerted scheme. Id. at 14. The Plaintiffs contend that the facts laid out in the Complaint allege with sufficient particularity one unified enterprise comprised of all the Defendants. Opp. p. 5. For the reasons below, the Court finds that the Plaintiffs have not sufficiently alleged one enterprise for purposes of a RICO violation.

An “enterprise” is defined as “a group of persons associated together for a common purpose of engaging in a course of conduct.” United States v. Turkette, 452 U.S. 576, 583 (1981). The definition of enterprise includes legal entities, such as corporations, associations or partnerships, and associations-in-fact. See 18 U.S.C. § 1961(4). The Plaintiffs attempt to satisfy the enterprise requirement by alleging that the Defendants formed an “association-in-fact” enterprise. This type of enterprise does not need to have a “hierarchical structure, a chain of command, or other business-like attributes,” but it must have “an ascertainable structure beyond that inherent in the pattern of racketeering activity in which it
engages.” *Boyle v. United States*, 556 U.S. 938, 955 (2009). “From the terms of RICO, it is apparent that an association-in-fact enterprise must have three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise’s purpose.” *Id.*

The Plaintiffs allege a classic “hub-and-spoke” type enterprise which occurs when there are separate, but bilateral, parallel, or vertical relationships between one central actor, the hub, and several independent actors at least one level removed from the hub, the spokes. Here, the Plaintiffs have alleged that Trilegiant acted as the hub and formed separate contracts with each E-Marketing Defendant, and they, in turn, relied on the help of each Credit Card Defendant to complete the chain. The Defendants argue that a hub and spoke type enterprise is not sufficient for a cause of action under RICO because the purported spokes are separate, uncoordinated, and entirely independent; thus there are no “relationships” between the spokes creating an ongoing and unified purpose.

MTD p. 13.

Hub-and-spoke enterprises have long been held by courts in this circuit to be insufficient as a matter of law to constitute the requisite enterprise for a RICO violation. *See City of N.Y. v. Chavez*, 944 F. Supp. 2d 260, 269-76 (S.D.N.Y 2013) (detailing historical treatment of Second Circuit courts finding these enterprises insufficient for RICO claims). In *Boyle*, however, the Supreme Court altered the analysis and directed courts to liberally and expansively interpret RICO’s
enterprise requirement by no longer requiring structural formality as a prerequisite. *Id.* at 270-271.

In the wake of *Boyle*, there has been no authoritative decision by the Second Circuit offering guidance as to how to interpret the enterprise requirement. The Third Circuit has, however, found that classic “hub and spoke” enterprises without allegations of a “rim” or “wheel” still do not sufficiently allege a RICO enterprise even post-*Boyle* because they do not, by definition, demonstrate that the “components function as a continuing unit.” *In re Ins. Brokerage Antitrust Litig.*, 618 F.3d 300, 327, 374-375 (3d Cir. 2010).

In *In re Insurance Brokerage Antitrust Litig.*, the court dismissed a RICO claim by several insured plaintiffs who alleged several broker-centered enterprises. *Id.* at 312. For each alleged enterprise, the plaintiffs accused one insurance broker of forming an agreement with one of several insurance providers to receive hidden brokerage fees for directing certain plaintiff purchasers to those providers. *Id.* The court found that because the plaintiffs failed to allege any cooperation between the insurance providers, the plaintiffs only described a pattern of uncoordinated parallel conduct by the providers, not a unified enterprise. *Id.* at 374-75. That court did acknowledge, however, that if a plaintiff pled agreement or organized cooperation between the spokes of the enterprise, it could allege a sufficient enterprise under RICO. *Id.* at 375-76. This analysis is consistent with the Supreme Court’s ruling in *Boyle*, especially since in that case the loosely knit, non-hierarchical core group of individuals, supplemented by recruits on occasion, met before each bank robbery to plan,
gather tools to commit, and assign roles for the commission of each crime. Therefore, even though no strict organization need be found, some structure showing agreement by the parties must be pled for a RICO claim to survive a motion to dismiss.

The Court also finds Judge Forrest’s analysis of the “hub and spoke” enterprise in *City of N.Y. v. Chavez*, particularly convincing and thorough. See *Chavez*, 944 F. Supp. 2d at 269-76 (finding that hub and spoke enterprises are no sufficient under RICO even post *Boyle*); *Neiman Marcus Group, Inc. v. Dispatch Trans. Corp.*, No. 09cv6861(NRB), 2011 WL 1142922, at *7 n.11 (S.D.N.Y. March 17, 2011) (finding hub-and-spoke enterprises “do not satisfy the enterprise element of a RICO claim”); *Conte v. Newsday, Inc.*, 703 F. Supp. 2d 126, 135 (E.D.N.Y. 2010) (finding that hub-and-spoke allegations are “insufficient to support a conclusion that the various defendants were associated with one another for a common purpose.”).\(^2\) This Court finds that a classic “hub-and-spoke” formation in which the spokes are separate, distinct and unassociated and whose actions are uncoordinated does not possess the requisite structure to constitute a RICO enterprise, even as that notion was expanded by *Boyle*, because there is no concerted effort or organized cooperation between the spokes.

Here, the Plaintiffs have alleged a series of commercial relationships between the E-Merchant Defendants, the Credit Card Defendants, and the

---

\(^2\) The Plaintiffs are correct that they do not need to allege a formal agreement to allege sufficiently an enterprise under RICO, but they must allege some type of informal cooperation or expectations of reciprocity to show that one enterprise exists. Opp. p. 13-14.
Trilegiant Defendants with the Trilegiant Defendants acting as the hub. CAC at ¶¶ 4-5, 8, 10-1, 72-87. There are no allegations that the spokes, comprised of the various E-Merchant Defendants and arguably the Credit Card Defendants, have any agreements or mutual expectations of reciprocal behavior. At best, the Plaintiffs have alleged a series of bilateral or possibly trilateral agreements between Trilegiant, one E-Merchant Defendant, and possibly one Credit Card Defendant for each alleged fraudulent transaction. Furthermore, there are no allegations that the various E-Merchant Defendants even knew the identity of the other E-Merchants. Similarly, there are no allegations that the Credit Card Defendants worked together to ensure a concerted effort to process membership fees for Trilegiant programs. Without allegations showing that these spokes worked in a concerted manner, the Plaintiffs have not sufficiently alleged an association-in-fact enterprise.

ii. Pattern of Racketeering Activity

The Defendants also move to dismiss the Plaintiffs’ RICO conspiracy claim, arguing that the Plaintiffs have not sufficiently alleged a pattern of racketeering activity. MTD p. 17-22.

To plead sufficiently a pattern of racketeering activity, the Plaintiffs must allege a pattern of “two or more predicate acts of racketeering” generally within a period of ten years. Lundy, 711 F.3d at 119 (citing 18 U.S.C. § 1961(5)); see also Curtis & Assocs., P.C. v. Law Offices of David M. Bushman, Esq., 758 F. Supp. 2d 153, 167-168 (E.D.N.Y. 2010). Section 1961(1) sets out an exhaustive list of

The Plaintiffs allege that the Defendants engaged in “predicate acts that constitute violations of the following statutes: (1) 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1341 (mail fraud); and 18 U.S.C. § 1344 (bank fraud),” and by “breaching (1) the settlement agreement they reached with 16 state attorneys general in December 2006, and (2) the settlement agreement they reached with former New York Attorney General Andrew M. Cuomo . . .” CAC at ¶¶ 157, 158. However, only Chase and Trilegiant are alleged to have been parties to the settlement agreements with the attorneys general.

1. Mail and Wire Fraud

The Defendants argue that the Plaintiffs fail to allege with sufficient particularity how the Plaintiffs were defrauded by the Defendants’ scheme, and without describing the alleged fraudulent activity in more detail, the Plaintiffs’ conclusory pleadings must be dismissed. MTD p. 18-21. In fact, they continue, the Plaintiffs do not sufficiently allege how any one mail or wire communication was fraudulent. Id. The Plaintiffs respond by arguing that they have sufficiently alleged a fraudulent scheme and that the Defendants used the mail and wires to
further that scheme. Opp. p. 28. They further argue that they are not required to
allege that any one instance of mail or wire fraud occurred as long as the
Defendants used those services in furthering the overall fraudulent scheme. Id.
at 29.

Where, as here, a RICO claim’s predicate acts include allegations based on
fraud, the circumstances constituting the alleged fraud must be pled with the
particularity required by Rule 9(b). Fed. R. Civ. Proc. 9(b); see also First Capital
Asset Mgmt., Inc. v. Santinwood, Inc., 385 F.3d 159, 178-179 (2d Cir. 2004).
Generally, a complaint based on fraudulent acts must “(1) specify the statements
that the plaintiff contends were fraudulent, (2) identify the speaker, (3) state where
and when the statements were made, and (4) explain why the statements were
fraudulent.” Mills v. Polar Molecular Corp., 12 F.3d 1170, 1175 (2d Cir. 1993); see
also Lerner v. Fleet Bank, N.A., 459 F.3d 273, 290 (2d Cir. 1993) (same); Eaves v.
addition to alleging factual particularity with respect to the fraudulent acts, “the
plaintiffs must allege facts that give rise to a strong inference of fraudulent
intent.” First Capital Asset Mgmt., 385 F.3d at 179. (quoting Moore v.
PaineWebber, Inc., 189 F.3d 165, 169 (2d Cir. 1999)). This is done by “(1) alleging
facts to show that defendants had both motive and opportunity to commit fraud,
or by (2) alleging facts that constitute strong circumstantial evidence of
conscious misbehavior or recklessness.” S.W.K.F.C., Inc. v. Bell Atl. TriCon
Leasing Corp., 84 F.3d 629, 633 (2d Cir. 1996).
Since the Plaintiffs allege that the Defendants used interstate “wire and mail communications for the purpose of executing and furthering [their] scheme to defraud Plaintiffs and other Class members,” they must plead with the requisite particularity detailed in Rule 9(b). CAC at ¶ 160. When discussing the use of interstate mail and wire communications, the Plaintiffs allege that the Defendants sent “thousands of electronic, mail and/or telephone communications” regarding various aspects of the scheme. Id. at 160(a)-(h). For the most part, however, they do not provide the contents of any of those communications, allege the dates and times of any of those communications, or allege the actual author of any of those specific communications. The only communications that have some detail are the credit card and debit account charges that the Credit Card Defendants sent to the Plaintiffs. Id. 160(h)(i)-(h)(xiv).

In DeSilva v. N. Shore-Long Island Jewish Health Sys. Inc., the court dismissed a RICO claim in which it was alleged that the defendants defrauded plaintiffs by systematically withholding “from plaintiffs their regular or statutorily required rate of pay for all hours worked.” DeSilva v. N. Shore-Long Island Jewish Health Sys. Inc., 770 F. Supp. 2d 497, 511 (E.D.N.Y. 2011). The plaintiffs in that case alleged that the defendants committed mail fraud by sending plaintiffs “thousand” of “payroll checks . . . that were ‘false and deceptive because they misled Plaintiffs and Class Members about the amount of wages to which they were entitled, the number of hours which they had worked, and whether the defendants had included all compensable time . . . .’” Id. The court found these
conclusory allegations insufficient to maintain a RICO claim because the plaintiffs “failed to identify which defendants caused each allegedly fraudulent statement to be spoken, written, or mailed; what the content of the allegedly fraudulent misrepresentation was; or when the communication was made.” *Id.* at 526. Instead, the “plaintiffs merely allege that unspecified defendants ‘repeatedly’ mailed payroll checks ‘on a regular basis . . . in the last 10 years.’” *Id.*

Similarly here, the Plaintiffs assert generalities, but fail to describe specifically how any mail or wire communication was used to enroll them in the Trilegiant membership programs. The Complaint asserts that “thousands” of communications were sent between the various Defendants without describing the contents or details of any one mail or wire communication that was fraudulent. The Plaintiffs instead rely on the hyperbolic conclusory allegation devoid of factual content asserting that the Defendants must have defrauded the Plaintiffs because they were engaged in various aggressive marketing and business tactics that resulted in the Plaintiffs’ unknowing enrollment into a membership program. In their roughly ninety page Complaint, the Plaintiffs do not specifically identify one false statement that a Defendant made to any Plaintiff related to enrolling in a Trilegiant membership program. On the other hand, the Plaintiffs admit that the Trilegiant offer page disclosed that Trilegiant practices negative option billing, but that this disclosure was in “exceedingly fine print.” CAC at ¶ 81. Even though they admit that there was a product offer page, they fail to describe any of the other conditions or omissions on that page. Without at
least alleging how any mail or wire communication was used to further the fraudulent scheme, let alone when the communication was made and by whom, the Plaintiffs have only provided the type of conclusory statements that Rule 9(b) is meant to preclude. See also In re Glenfeld Sec. Litig., 42 F.3d 1541, 1548 (9th Cir. 1994) (“plaintiff must set forth more than neutral facts necessary to identify the transaction. . . . In other words, the plaintiff must set forth an explanation as to why the statement or omission complained of was false or misleading.”), superseded by statute on other grounds as stated in SEC v. Todd, 642 F.3d 1207, 1216 (9th Cir. 2011).

To satisfy the particularity requirement of Rule 9(b), the Plaintiffs claim that they only need to detail the general contours of the RICO scheme and how the use of the mail and wires furthered that fraudulent scheme. Opp. p. 26. In In re U.S. Foodservice Inc. Pricing Litig., the court agreed and held that in complex fraud cases, the complaint does not need to allege the geographical and temporal details of every mail and wire transmission alleged to be a predicate act as long as the “defendant is on notice of the circumstances of the alleged fraud.” In re U.S. Food Service Inc. Pricing Litig., 2009 WL 5064468, at *18. The Plaintiffs’ allegations here though are substantially less detailed than the allegations in that case.

In In re U.S. Food Service, Inc., the plaintiffs alleged that the defendant enterprise “participated in a scheme to falsely inflate the cost component of the price charged to” the enterprise’s customers for certain goods. Id. at *17. As part of this scheme, the defendants agreed to artificially inflate the cost of the
goods through a series of purchases and sales among themselves. *Id.* The plaintiffs then relied on the defendants’ misrepresentations about their purchase price for the goods in agreeing to purchase the goods from the defendants for an inflated amount. *Id.* The plaintiffs alleged that the invoices and contracts that the resaler defendant sent them constituted the predicate acts of mail fraud under RICO because the invoices and contracts listed a fraudulent value for the goods. *Id.* In this instance, the court found that it did not need the plaintiffs to plead the specific dates and details of every invoice or contract because the “thousands of separate fraudulent transactions” only furthered the fraudulent scheme that the plaintiffs sufficiently pled. *Id.* at *18. In our case, however, the Plaintiffs have not even alleged how they were defrauded. Even drawing all reasonable inferences for the Plaintiffs at this stage, without alleging with some particularity how the Defendants defrauded them, the Court cannot find that the contours of the fraudulent scheme have been sufficiently alleged to justify relying on general allegations to sufficiently plead a pattern of racketeering activity.³

Finally, it is unclear to the Court based on the arguments and pleadings whether the Plaintiffs are alleging that datapass is inherently fraudulent or

³ The Plaintiffs also allege that as part of the fraudulent RICO scheme, the Credit Card Defendants sent “[t]housands of electronic or mail transmissions of credit or debit card statements to Plaintiffs and Class Members [that] contain the fraudulent charges.” CAC at ¶ 160(h). The Court is puzzled as to how these communications furthered the fraudulent scheme because they would have revealed, as they eventually did, not concealed the charges. See *Lundy*, 711 F.3d at 119-120 (mailing of pay stubs showing that the plaintiffs were underpaid was not in furtherance of a fraudulent scheme because the mailings would have revealed the alleged fraud). Moreover, credit card companies are legally required to send customers monthly statements of their charges. See 15 U.S.C. § 1666b. The Court doubts that the Plaintiffs intend to suggest that compliance with a federal consumer protection law constitutes a RICO violation.
whether it was an aspect of the mail and wire fraud discussed above. If the marketing scheme was meant to be included as an aspect of mail and wire fraud, it does not change the outcome of the Court’s conclusion because the Plaintiffs have not alleged the Defendants’ statements or omissions that defrauded them.

To the extent that the Plaintiffs allege that datapass is inherently fraudulent, their claims also fail because they have not told this Court why datapass is always fraudulent, despite the fact that a particular point in time some members of Congress concluded that certain unspecified practices labeled “datapass” were improper. For example, there are no allegations that datapass ineluctably results in automatic charges without the consumer’s knowledge and consent. Retailers constantly adapt to evolving legal mandates and market demands, and it is not alleged that datapass does not serve some potentially valid underlying sales purpose in helping willing consumers efficiently make online purchases. Without alleging with any particularity how the Plaintiffs were allegedly defrauded into purchasing the Trilegiant memberships, the Court cannot find that datapass is inherently fraudulent in this case.\footnote{The Plaintiffs rely on United States v. Warshank to support their claim that they have sufficiently pled the requisite particularity for a RICO claim. Opp. p. 33. In Warshank, the court confirmed a RICO criminal conviction for mail fraud when the defendants charged the plaintiffs for online purchases without informing the plaintiffs “during the ordering process that they would be charged for anything beyond the shipping-and-handling costs associated with the trial offer.” United States v. Warshank, 631 F.3d 266, 311 (6th Cir. 2010). Had the Plaintiffs here alleged that they were not told about the negative billing option or the membership program, the outcome of this motion might be drastically different. Unlike in Warshank, the Plaintiffs here have not alleged what they were and what they were not told. Without alleging these facts or omissions, the Court cannot determine how or even if the Defendants misrepresented the nature of the charges for the membership programs.} Moreover, without
detailed allegations describing what the Plaintiffs did and did not see and when, it is impossible to discern that the Plaintiffs were defrauded. See *Berry v. Webloyalty.com, Inc.*, No. 10-cv-1358-H(CAB), 2010 WL 8416525, at *5 (S.D. Cal Nov. 16, 2010) (customer error in failing to read the fine print or in failing to review the details of an online purchase does not convert the defendant’s actions into a pattern of racketeering activity).

2. **Bank Fraud**

The Defendants also argue that the Plaintiffs have no standing to allege predicate acts of bank fraud. MTD p. 23. The Plaintiffs failed to respond to the Defendants’ argument on this point. Given the law on this issue, it would appear that the Plaintiffs concede this point, as they do not expressly contest it, but the Court will address the merits regardless. To the extent that this claim still remains, the Plaintiffs cannot allege bank fraud as a predicate act under RICO. See *Chanof v. U.S. Surgical Corp.*, 857 F. Supp. 1011, 1023 (D. Conn. 1994) (dismissing claims in the pleadings because plaintiffs failed to respond to defendant’s motion to dismiss on these claims).

Bank fraud provides criminal liability for anyone who “knowingly executed, or attempts to execute, a scheme or artifice — (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises.” 18 U.S.C. § 1344. As the statute’s language makes patently clear, the bank fraud statute
protects financial institutions from being the victims of fraudulent activity. See *United States v. Chandler*, 98 F.3d 711, 715 (2d Cir. 1996) (finding that in the criminal context, “to obtain a bank fraud conviction under subsection (1) alone, the Government must prove beyond a reasonable doubt that the defendant engage[d] in or attempt[ed] to engage in a pattern or course of conduct designed to deceive a federally chartered or insured financial institution into released property”) (citations and internal quotation marks omitted); *United States v. Boceanu*, No. 07-cr-00012, 2013 WL 441072, at *2 (D. Conn. February 4, 2013) (finding that an element to prove a conspiracy to commit bank fraud includes an “agreement to engage in a scheme or artifice to defraud, or obtain money or property from, a federally-insured financial institution”); *Edmonds v. Seavey*, No. 08-cv-5646, 2009 WL 2949757, at *6 n.8 (S.D.N.Y. Sept. 15, 2009) (stating that “a RICO plaintiff who is not a financial institution under the statute lacks standing or injury to bring a RICO claim based on bank fraud”).

Here, the Plaintiffs do not allege that any financial institution was harmed. Conversely, the Plaintiffs allege that several financial institutions, or Credit Card Defendants, are part of the RICO enterprise engaged in defrauding the Plaintiffs. The Plaintiffs, therefore, may not rely on bank fraud as a predicate act.

3. **Breach of the Settlement Agreement**

The Defendants argue that the Plaintiffs cannot assert breaches of settlement agreements as predicate acts under RICO because breach of contract is not an enumerated predicate act. MTD p. 22-23. In response, the Plaintiffs
implicitly concede this point, but assert that “[w]hile breaching the settlement agreement is not one of the enumerated predicate acts that constitute racketeering activity as set forth in [the statute], it is one of the bases Plaintiffs have alleged to establish the Defendants’ fraudulent intent and a pattern of racketeering.” Opp. p. 32, n.23. From the Complaint and the Plaintiffs’ response, it is apparent that the alleged breaches are potentially used for two purposes: (1) as a substantive predicate act under the statute; and (2) to help prove the requisite fraudulent intent.

The list of predicate acts in 18 U.S.C. § 1961 is exhaustive. See O’Malley v. N.Y. City Transit Authority, 896 F.2d 704, 707-08 (2d Cir. 1990) (finding that state obstruction of justice is not a RICO predicate offense because it was not expressly listed in the statute); Binghamton Masonic Temple, Inc. v. Marin, 189 F.3d 460 (2d Cir. 1999) (unpublished opinion) (“As to the RICO claims, plaintiff lists numerous predicate acts, but amongst those only securities fraud, mail fraud, wire fraud and bank fraud are recognized predicate acts under RICO.”); Harvey v. Harvey, 931 F. Supp. 127, 130 (D. Conn. 1996) (“The offenses which may serve as predicate acts for a RICO claim are listed in 18 U.S.C. § 1961 . . . [and] [t]he list is exclusive.”). Since breaching a contract or, more specifically, a settlement agreement is not one of the offenses listed in 18 U.S.C. § 1961(1), it cannot serve as a predicate act to a RICO violation.5

5 Even though the Plaintiffs may have sufficiently pled the Defendants’ fraudulent intent to commit two predicate acts, the Court does not need to engage in this inquiry because the Plaintiffs have failed to allege sufficiently a pattern of racketeering activity to sustain a motion to dismiss.
iii. **RICO Statute of Limitations**

The Defendants also argue that any RICO claim brought by Plaintiffs Warfel, Reilly, and Restrepo are barred by the relevant statute of limitations. MTD p. 23-25. In response, the Plaintiffs argue that the statute of limitations was tolled because the Plaintiffs “suffered new and independent injuries with each imposition of a Trilegiant credit card charge on a class member, as the factual allegations of the CAC show that post-transaction marketing, data pass fraud, negative option billing and industrial scale ‘refund mitigation’ continued unabated for years until after these actions were filed.” Opp. p. 87.

Even though the RICO statute does not provide for a specific statute of limitations, the Supreme Court announced a uniform four-year limitations period for civil RICO actions. *See Agency Holding Corp. v. Malley-Duff & Assocs., Inc.*, 483 U.S. 143, 156-57 (1987). Although the Supreme Court has yet to specify when the RICO period of limitations begins to run, the Second Circuit has held that it “begins to run when the plaintiff discovers or should have discovered the RICO injury.” *In re Merrill Lynch P’ship Litig.*, 154 F.3d 56, 58 (2d Cir. 1998). “The first step in the statute of limitations analysis is to determine when the [plaintiff] sustained the alleged injury for which [the plaintiff] seek[s] redress. [The Court] then determine[s] when [the plaintiff] discovered or should have discovered the injury and begin[s] the four-year statute of limitations period at that point.” *Id.* at 59 (citations and internal quotation marks omitted).
The Second Circuit also “recognizes a ‘separate accrual’ rule under which a new claim accrued and the four-year limitation period begins anew [for a civil RICO claim] each time a plaintiff discovers or should have discovered a new and independent injury.’” Id. at 58. As other courts in this circuit have noted, the case law “leaves some ambiguity as to precisely what constitutes a ‘new and independent injury.’” Republic of Colombia v. Diageo N. Am. Inc., 531 F. Supp. 2d 365, 448 (E.D.N.Y. 2007) (citations omitted).

1. Date of the Injury

First, the Court must determine when the alleged injury occurred. According to the Complaint, Plaintiff Warfel was enrolled in one of Trilegiant’s monthly membership programs in or around December 2004; Plaintiff Reilly was enrolled in one of Trilegiant’s monthly membership programs in or around May 2007; and Plaintiff Restrepo was enrolled in one of Trilegiant’s membership programs on May 9, 2007. CAC at ¶¶ 27, 28, 33. Each of the Plaintiffs also alleges that they were shortly thereafter charged monthly fees for the Trilegiant memberships. Id. The Plaintiffs argue, however, that each monthly charge constituted a new and independent injury under the separate accrual doctrine. Opp. 87. The Court disagrees with this contention.

The facts of this case are substantially similar to those in In re Merrill Lynch Partnerships Litig., and warrant a finding that no new and independent injury occurred after the initial membership enrollment. In that case, the plaintiffs alleged that the defendant scammed real estate investors into purchasing
ownership interests in a series of limited partnerships even though the defendant knew that the partnerships could not make the advertised gains. In re Merrill Lynch Partnerships Litig., 154 F.3d at 57-58. The defendant was alleged to have sold the investments hoping to “collect significant fees during the course of the partnership life.” Id. at 59. The plaintiffs alleged they sustained new and independent injuries every time the defendant collected annual partnership fees and every time they received marketing materials designed to reinsure the investors of the strength of their investments. Id. The court found, however, that “later communications, which put a gloss on the losing investments, were continuing efforts to conceal the initial fraud, and not separate and distinct fraudulent acts resulting in new and independent injuries.” Id. at 60. Similarly, “the collection of annual fees [that] occurred in each year of the life of the partnerships . . . cannot be viewed as a separate and distinct fraud creating new injuries as it was simply a part of the alleged scheme.” Id. at 60.

The Plaintiffs unavailingly rely on AMA v. United Healthcare Corp. In that case, the defendant healthcare company was accused of continually manipulating the databases responsible for establishing reimbursement rates for out-of-network reimbursement claims. AMA v. United Healthcare Corp., No. 00 Civ. 2800(LMM), 2006 WL 3833440, at *2 (S.D.N.Y. Dec. 29, 2006). The court found that each time a new reimbursement rate was determined, the plaintiffs suffered a new and independent injury. Id. at *10. Important for that determination was the fact that the new reimbursement rates were themselves fraudulent. The Plaintiffs here have only alleged that they were fraudulently enrolled into a membership
program that automatically charged them monthly dues based on the billing
information provided by the Credit Card Defendants. The charges appeared
accurately and timely on each of the Plaintiff's credit card or debit account
statements. Unlike in *AMA v. United Healthcare Corp.*, the Defendants committed
no other continuing fraudulent actions related to the initial scheme that would
cause new and independent injuries. Instead, once the Plaintiffs were enrolled in
the membership, the initial fraudulent part of the alleged RICO scheme was
completed.

Here, the facts are more akin to *In re Merrill Lynch Partnerships Litig.* The
Plaintiffs allege that they were fraudulently induced to enroll in Trilegiant's
membership programs through a complex scheme involving several questionable
business practices. CAC at ¶¶ 74-87. The scheme resulted in the Plaintiffs'
enrollment in one of the membership programs without their explicit
authorization or consent. Each Trilegiant membership charge later collected was
simply one in a series of charges unwittingly authorized by and incident to the
initial enrollment.

As the Plaintiffs concede, negative option billing is used to make
“[a]ffirmative consumer action . . . impossible” until consumers become aware
that they have been enrolled in the membership program, which “does not occur
until months, if not years, after Trilegiant first begins to charge recurring
membership fees.” CAC at ¶ 82. Refund mitigation, furthermore, is used only to
“minimize the amount of improper charges [Trilegiant] would have to refund to . .
. consumers who eventually discover that they have been unknowingly enrolled
in the Membership Programs and charged unauthorized monthly fees.” CAC at ¶ 83. This post-enrollment conduct was not used to create new and independent RCO-related injury, but was meant to conceal and further the initial fraud.

2. **Knowledge or Constructive Knowledge**

Second, the Court now must determine when the Plaintiffs discovered or should have discovered the injury. In the Second Circuit, actual knowledge of the fraudulent scheme is not necessary; an objective standard is used to impute knowledge to the victim when sufficient “storm clouds” are raised to create a duty to inquire. *See Dodds v. Cigna Secs., Inc.*, 12 F.3d 346, 350 (2d Cir. 1993) ("'[t]he means of knowledge are the same thing in effect as knowledge itself,' and, therefore, ‘when the circumstances would suggest to a [person] of ordinary intelligence the probability that she has been defrauded, a duty of inquiry arises, and knowledge will be imputed to the [plaintiff] who does not make such an inquiry.’") (quoting *Armstrong v. McAlpin*, 699 F.2d 79, 88 (2d Cir. 1983)). Since inquiry notice is a factual examination, “making this determination is frequently inappropriate on a motion to dismiss and is only proper . . . when the complaint and documents which the court may take notice of clearly show that the claims are barred as a matter of law.” *Lorber v. Winston*, No. 12-cv-3571(ADS)(ETB), 2013 WL 3424173, at *20 (E.D.N.Y. July 3, 2013) (citations and internal quotation marks omitted). Importantly, the storm warnings “need not detail every aspect of the alleged fraudulent scheme,” but must suggest to a person of ordinary intelligence the probability of fraudulent activity. *Staehr v. Hartford Fin. Servs. Grp., Inc.*, 547
In this case, the Plaintiffs admit that after they were enrolled in Trilegiant’s membership programs, they received “credit or debit card statements... containing the fraudulent charges.” CAC at ¶ 160(h). However, they allege that they only “noticed the recurring charges” years after the initial enrollment. CAC at ¶¶ 27-29, 33. The Plaintiffs claim, therefore, that they had no actual or constructive knowledge of the fraudulent activity. The Court, drawing all inferences in favor of the Plaintiffs, finds that the Plaintiffs did not have actual knowledge of the injury at the time of enrollment. The question before this Court, then, is when the Plaintiffs were on sufficient inquiry notice of the scheme to start running the statute of limitations.

Since the Plaintiffs admit that they received credit card or debit account statements accurately reflecting the amounts charged for the membership programs shortly after enrolling in the programs, the Court must determine if this placed them on sufficient inquiry notice of the alleged scheme. In a case brought under the Truth in Lending Act, in which a president of a company sought reimbursement for what he alleged were unauthorized charges by one of his employees on the corporate credit card, the Second Circuit found that the credit card company was not liable for reimbursement. Minskoff v. Am. Express Travel Related Servs. Co., Inc., 98 F.3d 703, 708-10 (2d. Cir. 1996). Importantly, the court stated that “once a cardholder receives a statement that reasonably puts him on notice that one or more fraudulent charges have been made, he cannot thereafter

In *Dodds*, the court found that the inexperienced-investor plaintiff was on inquiry notice that she may have been defrauded by her investment manager because she had access to the prospectuses of the companies in which he proposed to invest. *Dodds*, 841 F. Supp. at 94. The court stated that a person of ordinary intelligence would have been put on inquiry notice through these materials, and the plaintiff’s claims that she did not read the documents because they were overly complex were unavailing because “[a] plaintiff is not free to ignore pertinent documents even if she is not able to fully understand their meaning.” *Id.*

Accordingly, this Court follows the general consensus in this circuit and finds that receiving credit card statements, far less impenetrable than corporate securities filings, should have given the Plaintiffs sufficient inquiry notice of the fraudulent scheme. Indeed, the Plaintiffs own allegations prove this to be true because the Plaintiffs only discovered the charges after eventually reviewing their credit card or debit card statements. CAC at ¶¶ 24-34. Had the Plaintiffs
reviewed their credit card statements earlier than when they finally did, they would have been aware of the charges.

In the Complaint, Plaintiff Warfel admitted that around December 2004, she was enrolled in a Trilegiant membership program and the monthly charges commenced “[s]oon thereafter.” CAC at ¶ 33. Warfel’s initial complaint was filed in the Southern District of Ohio on August 4, 2011, more than six years after she should have known of the injury. Opp. p. 83. Her RICO claims, therefore, would be barred by the statute of limitations.

Plaintiff Reilly was enrolled in a Trilegiant membership program around May 2007. CAC at ¶ 27. Reilly filed a complaint on March 7, 2012, more than four years after he should have known of the injury. His RICO claims, therefore, would be barred by the statute of limitations.

Finally, Plaintiff Restrepo claimed that on “May 9, 2007, Trilegiant Charged” his Chase MasterCard. CAC at ¶ 28. Restrepo’s initial claim was filed on July 13, 2011 in the District of Arizona, just over four years after the initial charge. Even assuming that the charges did not appear until his June statement, his RICO claims would still be barred by the statute of limitations.

For the foregoing reasons, the Court finds that the Defendants’ motion to dismiss the Plaintiffs’ substantive RICO claims is GRANTED, and it is so ordered.

b. Conspiracy to Violate RICO, 18 U.S.C. § 1962(d)

The Defendants also move to dismiss the Plaintiffs’ claim for a conspiracy to violate RICO because (1) the Plaintiffs have failed to sufficiently plead a substantive RICO violation; and (2) the Plaintiffs failed to allege any agreement by
the Defendants. MTD p. 25-27. The Plaintiffs respond by arguing that they are not required to plead all of the elements of a substantive RICO violation for a conspiracy cause of action, and they have sufficiently alleged an agreement of the conspiracy through each participant’s knowledge of the RICO scheme. Opp. 44-59.

The RICO statute makes it unlawful for “any person to conspire” to violate RICO. 18 U.S.C. § 1962(d). To establish a conspiracy claim pursuant to this statute, a “plaintiff must establish ‘as to each alleged co-conspirator: (1) an agreement to join the conspiracy; (2) the acts of each co-conspirator in furtherance of the conspiracy; [and] (3) that the co-conspirator knowingly participated in the same.” Valenti v. Penn. Mut. Life Ins. Co., 850 F. Supp. 2d 445, 450-451 (S.D.N.Y. 2012), aff’d, 511 F. App’x 57 (2d Cir. 2013) (citations omitted); United States v. Pizzonia, 577 F.3d 455, 463 (2d Cir. 2009) (a RICO conspiracy requires allegations that the defendant agreed to participate “in a charged enterprise’s affairs’ through a pattern of racketeering, ‘not a conspiracy to commit predicate acts.’”) (quoting United States v. Persico, 832 F.3d 705, 714 (2d Cir. 1987)); N.Y. Dist. Council of Carpenters Pension Fund v. Forde, No. 11 Civ. 5474(LAP), 2013 WL 1454954, at *10 (S.D.N.Y. Mar. 26, 2013) (“To establish a RICO conspiracy, a plaintiff must plead that a defendant agreed to participate in the affairs of the enterprise through a pattern of racketeering activity.”).

In this circuit, analysis of any RICO conspiracy claim begins with the premise that it necessarily fails where the underlying substantive claim is insufficiently pled. See First Capital Asset Mgmt., Inc. 385 F.3d at 182; Ozbakir v.
Scotti, 764 F. Supp. 2d 556, 573-74 (W.D.N.Y. 2011) (“To the extent that plaintiffs seek to assert a RICO conspiracy claim under 18 U.S.C. § 1962(d), such a claim also fails, because it is based on the defectively pleaded substantive RICO Claims.”); Allen v. New World Coffee, Inc., No. 00-cv-2610, 2002 WL 432685, at *6 (S.D.N.Y. March 19, 2002) (“Any claim under § 1962(d) based on conspiracy to violate the other subsections of section 1962 must fail if the substantive claims are themselves deficient.”) (quoting Discon, Inc. v. NYNEX Corp., 93 F.3d 1055, 1064 (2d Cir. 1996), vacated on other grounds, 525 U.S. 128 (1998)); Denny v. Ford Motor Co., 959 F. Supp. 2d 262, 274 (N.D.N.Y. 2013) (“Because plaintiffs’ substantive RICO claims are untimely, their conspiracy to violate RICO claim must fail as a matter of law.”).

The Plaintiffs do not directly respond to the Defendants’ argument on this point. Accordingly, the Plaintiffs claim for a RICO conspiracy must be dismissed because they have failed to allege sufficiently a substantive RICO violation as discussed supra.6

Even so, the Plaintiffs’ RICO conspiracy claim fails for independent reasons. If the Plaintiffs do not need to allege an actual enterprise to fulfill the requirements for a RICO conspiracy claim, they must at the very least allege an agreement to commit the predicate acts. See Hecht v. Commerce Clearing

6 Even if the Plaintiffs are not required to allege an enterprise for a RICO conspiracy claim, they have not sufficiently alleged a pattern of racketeering activity or even an agreement to commit such acts. For those independent reasons, the Complaint is insufficient. See United States v. Applins, 637 F.3d 59, 75 (2d Cir. 2011) (finding that a RICO enterprise does not need to be proved beyond a reasonable doubt to sustain a RICO conspiracy conviction).
House, Inc., 897 F.2d 21, 25 (2d. Cir. 1990) (“Because the core of a RICO civil conspiracy is an agreement to commit predicate acts, a RICO civil conspiracy complaint, at the very least, must allege specifically such an agreement.”); Book v. Mortg. Elec. Registration Sys., 608 F. Supp. 2d 277, 282 (D. Conn. 2009). Here, the Plaintiffs allege in a conclusory fashion that the “Defendants agreed with each other to enter into a conspiracy to, and did, in fact, conduct and participate in the affairs of the RICO Enterprise, directly or indirectly, through a pattern of racketeering activity.” CAC at ¶ 176. The Plaintiffs never allege, however, how or when all of the Defendants formed such an agreement. The Plaintiffs explicitly allege the existence of agreements between Trilegiant and each E-Merchant Defendant and between Trilegiant and some Credit Card Defendants, as related to separate marketing initiatives, but they do not allege one agreement where all of the Defendants conspired together to engage in one fraudulent scheme. CAC at ¶¶ 5-8, 83-87, 103, 117. All the Plaintiffs have done is “taken a series of events involving various individuals and entities, and various communications among them, and attempted to ‘connect the dots,’ hoping that when they finish, a RICO claim will emerge. The federal rules of pleading have been designed to discourage such attempts . . . .” Ozbakir, 764 F. Supp. 2d at 573.

The Plaintiffs argue that at the pleading stage, they must only allege that the co-conspirators knew the general nature and contours of the conspiracy, not that they actually had any agreement to commit RICO violations. Opp. p. 46. The cases the Plaintiffs cite, however, do not stand for the proposition that the only requirement to allege sufficiently a RICO conspiracy is knowledge of it. For
example, in *United States v. Zichetello*, the court addressed whether co-conspirators needed to know and agree to the racketeering activity of the enterprise for the government to sustain a RICO conspiracy conviction. *United States v. Zichetello*, 208 F.3d 72, 99 (2d Cir. 2000). The court held that the government did not need to prove that each co-conspirator agreed to commit all of the predicate acts, instead, “[a]ssuming that a RICO enterprise exists, the government must only prove that the defendant[s] . . . know the general nature of the conspiracy and that the conspiracy extends [their] individual role[s].” *Id.* (citations and internal quotation marks omitted). The court’s analysis was explicitly based on the assumption that “a RICO enterprise exists.”

When a plaintiff sufficiently alleges an enterprise, they allege by definition an explicit or implicit agreement among the defendants. Here, however, the Plaintiffs have not sufficiently alleged an enterprise. Moreover, the Plaintiffs are attempting to allege, it seems, that mere knowledge of a conspiracy’s actions makes the person with that knowledge liable as a co-conspirator. Knowledge alone cannot be enough to subject a person to criminal and civil liability for conspiracy. Without alleging an agreement, the Plaintiffs cannot show that the Defendants have in fact agreed to conspire together to violate RICO.

Finally, the Plaintiffs’ RICO conspiracy claim also fails because the allegations therein “contain no more specificity than the other allegations in the complaint.” *Ozbekir*, 764 F. Supp. 2d at 574 (dismissing a RICO conspiracy claim because the substantive RICO violation was not sufficiently pleaded, and the RICO conspiracy allegations contained no more specificity than the substantive
RICO allegations). Therefore, the Complaint has not complied with the heightened requirements of Rule 9(b) even though it relies on a pattern of racketeering activity based on fraud.

For the foregoing reasons, the Defendants’ motion to dismiss the RICO conspiracy claims is GRANTED.


The Trilegiant and E-Merchant Defendants move to dismiss the Plaintiffs’ ECPA claims because the Plaintiffs have failed to allege that the interception occurred contemporaneously to the communications’ transmissions, and, in the alternative, that several of the Plaintiffs’ claims are barred by the relevant statute of limitations. MTD p. 27-29. The Plaintiffs argue that they are not barred by the statute of limitations because they were not put on notice of the violation, and they have sufficiently alleged interceptions for purposes of the statute. Opp. 89-96. For the reasons set forth below, the Court finds that some of the Plaintiffs’ claims are not barred by the statute of limitations and that the Complaint adequately asserts a violation of ECPA.

i. ECPA “Interception”

ECPA provides a civil cause of action against persons who intentionally intercept, endeavor to intercept, or procure others to intercept electronic communications. 18 U.S.C. §§ 2511. Courts addressing the term “intercept” have narrowly defined it to encompass only “‘acquisitions of communications contemporaneous with transmission, not storage.’” Snyder v. Fantasy
Interactive, Inc., No. 11-cv-3593(WHP), 2012 WL 569185, at *2 (S.D.N.Y. Feb. 9, 2012); Conte v. Newsday, Inc., 703 F.Supp.2d 126, 139 at n. 11 (E.D.N.Y. 2010); Knop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); see also, Fraser v. Nationwide Mut. Ins., Co., 352 F.3d 107, 113-14 (3rd Cir. 2003) (following Fifth, Ninth, and Eleventh Circuits and interpreting intercept narrowly); United States v. Meriweather, 917 F.2d 955, 960 (6th Cir. 1990). While the Second Circuit has yet to rule definitively on this issue, it has implied in dictum that it is not persuaded that an interception of a wire or communication can only occur while the communication is in “transit.” See Hall v. Earthlink Network, Inc., 396 F.3d 500, n.1 (2d Cir. 2005).

For purposes of this motion to dismiss, however, the Court does not need to decide whether an interception must be contemporaneous to the communication’s transit because even assuming the Defendants’ standard is correct, the Plaintiffs have sufficiently alleged the temporal requirement. Several Plaintiffs have claimed that while making purchases on the E-Merchant Defendants’ websites, they entered their confidential billing information which was then stored in an online token to be transferred to Trilegiant at some point in the transaction. CAC at ¶ 117. After entering their account information, the Plaintiffs were taken to Trilegiant’s offer page to complete a secondary purchase without receiving confirmation that the first transaction was completed. CAC at ¶¶ 74, 117. They would only receive confirmation of their initial purchase after reviewing Trilegiant’s offer page. CAC at ¶¶ 74, 117. Based on the allegations, and drawing all inferences in favor of those allegations, the Plaintiffs have alleged
two alternative “interceptions.” The first could have occurred when the token stored the Plaintiffs’ confidential billing information. See 18 U.S.C. § 2511(2)(d); Caro v. Weintraub, 618 F.3d 94, 97-98 (2d Cir. 2010) (finding that a party to a communication can intercept the communication if it clandestinely records a conversation with the intention to commit a tort or other crime with the intercepted communication). That interception would have occurred the moment the Plaintiffs sent their billing information to the E-Merchant Defendant; thus, occurring contemporaneously to the communication’s transmittal. An interception does not require immediate use of the intercepted information, so the fact that the token may have only saved the data is irrelevant. The second interception could have been when the billing information was sent to Trilegiant. Even though other courts have interpreted interception “narrowly,” they were only distinguishing between communications that were either in transit or in storage. See Konop, 302 F.3d 868 at 878-79. Here, the Plaintiffs’ confidential billing information would not have been “in storage” until after the entire transaction with the E-Merchant was completed, and an online purchase is completed only when the customer receives a purchase confirmation page from the vendor. Before that time, the communications related to the transaction are not “in storage” and, therefore, are more properly defined as in a state of transit. Accordingly, the Plaintiffs have sufficiently alleged that the communications were intercepted contemporaneously to their transmissions and have sufficiently alleged violations of ECPA.
ii. **ECPA Statute of Limitations**

The Defendants also argue that several of the Plaintiffs’ ECPA claims are barred by the relevant statute of limitations. Neither party contests that the applicable statute of limitations for an ECPA claim is “two years after the date upon which the claimant first had a reasonable opportunity to discover the violation.” 18 U.S.C. § 2520(e); see also *In re State Police Litig.*, 888 F. Supp. 1235, 1248-249 (D. Conn. 1995); *Schmidt v. Devino*, 106 F. Supp. 2d 345, 349-50 (D. Conn. 2000). Courts in this district have held that the merest inquiry notice is sufficient to start the statute of limitations running absent allegations of fraudulent concealment. *Id.*

Even though the “violation” that is referenced in the statute is the interception of the communication, not the injury caused by the interception, the Plaintiffs only need to be on inquiry notice of the violation to commence the statute of limitations period. Contrary to the Plaintiffs’ contentions, they did not need to be on notice of the actual violation, just on notice to inquire about the injury they had received. The credit card and debit account statements should have alerted the Plaintiffs that “something was afoot.” *See Davis v. Zirkelbach*, 149 F.3d 614, 618 (7th Cir. 1998). Had they inquired about the injury, they would have discovered the alleged violation. Since the Court has already held that the Plaintiffs’ financial statements were sufficient to put them on inquiry notice, it must only determine when the Plaintiffs first received their statements with the relevant membership charges.
Plaintiff Kelm alleges that shortly after June 2009, her credit card was charged for a membership fee. CAC at ¶ 25. Plaintiff Pham alleges that from January 11, 2010 to August 11, 2011, her credit card was charged for monthly membership fees. CAC at ¶ 26. Plaintiff Reilly alleges that shortly after May 2007, his credit card was charged for a membership fee. CAC at ¶ 27. Plaintiff Restrepo alleges that on May 9, 2007, his credit card was charged for a membership fee. CAC at ¶ 28. Plaintiff Brian Schnabel alleges that on or about December 20, 2007, his credit card was charged a membership fee. CAC at ¶ 29. Plaintiff Warfel alleges that shortly after December 2004, her credit card was charged a membership fee. CAC at ¶ 33. Finally, Plaintiff Williams alleges that in August 2009, her debit card was charged a membership fee. CAC at ¶ 34. All of these Plaintiffs alleged they received membership charges more than two years prior to filing their relevant complaints, and none of these Plaintiffs allege any irregularity in the customary posting of credit card charges; therefore, the Court construes the Complaint to allege that the Trilegiant membership fee appeared on the Plaintiffs’ credit card statements issued in the month immediately following their enrollment in the Trilegiant membership program. Accordingly, their ECPA claims are barred by the statute of limitations.

The Defendants’ motion to dismiss the ECPA claims asserted by Plaintiffs Kelm, Pham, Reilly, Restrepo, Brian Schnabel, Warfel, and Williams against the Trilegiant and E-Merchant Defendants is GRANTED as barred by the statute of limitations; while the motion to dismiss those claims asserted by the Plaintiffs DiCarolis, Edward and Lucy Schnabel, Sumlin, and Timmcke is DENIED.
d. **Claims for Violations of CUTPA, Conn. Gen. Stat. § 42-110a, et seq.**

The Defendants first move to strike the pleadings as related to the CUTPA class action claim on the ground that CUTPA does not allow for a class action when a Connecticut resident is not a named plaintiff. MTD p. 32-33. The Defendants also move to dismiss the CUTPA claim arguing that the Plaintiffs have not sufficiently alleged a substantive CUTPA violation and that several claims are barred by the relevant statute of limitations. MTD p. 33-36. The Plaintiffs argue that (1) the motion to strike is untimely and procedurally improper; (2) Rule 23 supersedes the class restrictions in CUTPA; and (3) the Plaintiffs have sufficiently alleged CUTPA claims that are not barred by the statute of limitations. Opp. p. 96-114.

i. **Defendant’s Motion to Strike**

This Court finds that: (1) the motion to strike is procedurally proper; (2) CUTPA does not allow for national class actions; and (3) Rule 23 does not supersede the class restrictions in CUTPA.

1. **Procedural Posture**

Rule 12(f) provides that a “court may strike from a pleading any insufficient defense or any redundant, immaterial, impertinent or scandalous matter.” Fed. R. Civ. P. 12(f). Motions to strike “are not favored and will not be granted unless it is clear that the allegations in question can have no possible bearing on the subject matter of the litigation.” *Schramm v. Kirschell*, 84 F.R.D. 294, 299 (D. Conn. 1979). Allegations are immaterial if they have “no essential or important relationship to
the claim for relief or the defenses being pleaded.” *Mahon v. Chicago Title Ins.* Co., No. 3:09cv690(AWT), 2009 WL 4268372, at *1 (D. Conn. Nov. 24, 2009) (citations and internal quotation marks omitted); see also *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887, 893 (2d Cir. 1976).

Rules 23(a) and 23(b) provide the procedural bases for determining the appropriateness of class certification. See Fed. R. Civ. P. 23(a)-(b). Rule 23(a) lists the prerequisites of numerosity, commonality, typicality, and adequacy of representation. Fed. R. Civ. P. 23(a). Rule 23(b) indicates that a “class action may be maintained if Rule 23(a) is satisfied and if” either: (1) separate actions would create a risk of inconsistent adjudications or adjudications that would impair the interests of other nonparty class members; (2) “the party opposing the class has acted or refused to act on grounds that apply generally to the class;” or (3) “the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b).

In *Rogers v. Capital One Servs., LLC*, this Court articulated the standard for striking class allegations prior to a motion for certification.

A court may grant a motion to strike and order deletion of portions of a complaint’s class claims where the basis for the motion to strike is distinct from the issues that would be decided in connection with determining the appropriateness of class certification under Rules 23(a) and 23(b) of the Federal Rules of Civil Procedure and it is clear that plaintiffs cannot possibly prove the deleted portions of those claims.
In *Rogers*, this Court denied a motion to strike class allegations where the defendants argued that “the proposed class could not be certified” because individual questions would predominate over common issues of law, and “the predominance criterion is a Rule 23(b) requirement, and therefore is not a proper basis for a motion to strike class allegations.” *Rogers*, 2011 WL 873312, at *9.

In *Rahman*, on the other hand, the court granted a motion to strike class allegations because the issue of “the extent to which the claims of absent members of the putative class have been exhausted” was “separate and apart from the issues that [would] be decided on a class certification motion.” *Rahman*, 2008 WL 161230, at *3.

In this case, the Defendants’ main challenge to the class allegations in the Complaint is that “CUTPA explicitly precludes individuals who do not reside in Connecticut from bringing claims on behalf of a class.” MTD p. 32. This alleged bar to the class proceeding, therefore, is a statutory restriction unrelated to the issues to be addressed at the class certification stage, i.e. those listed in Rules 23(a) and 23(b). Furthermore, the availability for a foreign named plaintiff to represent a class under CUTPA is a matter of law and can be determined on the facts of the Complaint. Therefore, this Court need not wait until a motion for class certification to strike class allegations on this basis.
In support of their argument that striking class allegations is procedurally improper at this stage, the plaintiffs cite Chenensky v. N.Y. Life Ins. Co., in which the court stated that a “motion to strike class allegations . . . is even more disfavored because it requires a reviewing court to preemptively terminate the class aspects . . . before plaintiffs are permitted to complete [] discovery . . . on questions relevant to class certification.” Chenensky v. N.Y. Life Ins. Co., No. 07 CIV. 11504(WHP), 2011 WL 1795305, at *1 (S.D.N.Y. Apr. 27, 2011) (quoting Ironforge.com v. Paychex, Inc., 747 F. Supp. 2d 384, 404 (W.D.N.Y. 2010)). However, the issues raised in the defendant’s motion to strike in Chenensky were that “individual issues predominate; the class lacks commonality and typicality; and [the plaintiff was] not an adequate class representative.” Id. at *2. All of these issues fall under the Federal Rules of Civil Procedure 23(a) and 23(b) analysis, and, as described above, would more properly be decided on a class certification motion. The Defendants here do not allege any issues that would be determined under a Rule 23(a) and (b) analysis.

For those reasons, the Court views the motion to strike as procedurally proper at this stage of the litigation.

2. CUTPA’s Class Action Restriction

CUTPA creates both individual and class causes of action. The statute provides:

(a) Any person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b, may bring an action in the judicial district in which the plaintiff or defendant resides or has his principal place of business or is doing business,
to recover actual damages. Proof of public interest or public injury shall not be required in any action brought under this section. The court may, in its discretion, award punitive damages and may provide such equitable relief as it deems necessary or proper.

Conn. Gen. Stat. § 42-110g(a). That section confers a right of action to an individual plaintiff harmed by unfair or deceptive trade practices to bring an action in Connecticut. Subsection (b) of that section limits that right of a person to bring a class action by stating that:

Persons entitled to bring an action under subsection (a) of this section may, pursuant to rules established by the judges of the Superior Court, bring a class action on behalf of themselves and other persons similarly situated who are residents of this state or injured in this state to recover damages.

Conn. Gen. Stat. § 42-110g(b). The statute permits any person authorized to bring a CUTPA action on their own behalf to bring a class action only on behalf of similarly situated residents of Connecticut or those that were injured in Connecticut.

The Defendants argue that the Court should strike the Plaintiffs national class action claims under CUTPA because the Plaintiffs “who do not reside in Connecticut and were not injured in Connecticut” are explicitly precluded from “bringing claims on behalf of a class.” MTD p. 32. The Plaintiffs urge the Court to read the statute to permit a class action to be brought on behalf of persons who do not reside in Connecticut and who were not injured in Connecticut. The Plaintiffs do not argue that the language is ambiguous, but rather argue on public policy grounds that, although they are not residents and were not injured in Connecticut, they should be allowed to bring a class action suit under CUTPA
because there is a sufficient nexus to Connecticut: (1) the Plaintiffs allege that the headquarters of both Trilegiant and Affinion are located in Norwalk, Connecticut;” and (2) “from this headquarters, Trilegiant and Affinion designed and implemented their data pass scheme, intercepted consumers’ billing information, and initiated unauthorized charges against consumers’ accounts.” Opp. p. 99.

“The meaning of a statute shall, in the first instance, be ascertained from the text of the statute itself and its relationship to other statutes. If, after examining such text and considering such relationship, the meaning of such text is plain and unambiguous and does not yield absurd or unworkable results, extratextual evidence of the meaning of the statute shall not be considered.” Conn. Gen. Stat. § 1-2z. Furthermore, it is incumbent upon a party seeking an interpretation of a statute in variance with its apparently plain meaning to identify some ambiguity in the language itself, some ambiguity in the statute’s context, or something in the legislative history of the statute suggesting the interpretation it espouses. F.D.I.C. v. Calderallo, 79 Conn. App. 384, 394-96 (2003). In any event, Courts are obliged to construe statutes in a manner which effectuates the legislative intent. Lauer v. Zoning Comm’n, 220 Conn. 455, 459–60 (1991). “A court should accord a statutory enactment its plain meaning” when its apparent meaning is not called into question as it was in Courchesne. State v. Jimenez, 228 Conn. 335, 341 (1994); Kilpatrick v. Bd. of Educ. of Town of Fairfield, 206 Conn. 25, 28 (1988).

The Plaintiffs offer no alternative interpretation of the language of the statute, and no other legislative history or contextual support for the
interpretation they advocate. Instead, they challenge the wisdom of the language and assert that because there is a nexus to the state the legislature should have allowed Connecticut residents to bring class actions on behalf of nonresidents. In essence, the Plaintiffs ask this Court to supplant its judgment for that of the legislature rather than to interpret the legislature’s intent. That is not the role of a Court. Were the Court to conduct the standard statutory analysis, it would find that the language clearly and unambiguously does not permit a class action to be brought on behalf of non-residents or on behalf of those not injured in Connecticut, and that the language expresses the deliberate legislative intent that such suits not be permitted, as reflected in the legislative history discussed infra.

Further, a court in this district has held that a “foreign person suffering ascertainable loss outside of Connecticut from unlawful conduct occurring inside the state may initiate an individual action in Connecticut, but may not bring a class action because such plaintiff could not be representative of class members with the statutorily required in-state residency or injury characteristics.” Metro. Enter. Corp. v. United Techs. Int’l, Corp., Pratt & Whitney Large Commercial Engines Div., No. 3:03CV1685(JBA), 2004 WL 1497545 (D. Conn. June 28, 2004). In Metro. Enter. Corp., the court denied a motion to dismiss an individual CUTPA claim by a nonresident injured outside of Connecticut while indicating that the nonresident plaintiff could not have brought a class action suit. See also Macomber v. Travelers Prop. & Cas. Corp., 277 Conn. 617, 624 (Conn. 2006) (“It is possible that this provision bars a national class action for CUTPA violations, such as this case.”).
In this case, none of the named Plaintiffs are Connecticut residents, and none of the Plaintiffs were injured in Connecticut. Therefore, the terms of CUTPA and the state’s jurisprudence prohibit the Plaintiffs from bringing a class action on behalf of a national class.

3. CUTPA and Rule 23

The Plaintiffs next argue that even if the terms of CUTPA would bar their national class, Rule 23 supersedes CUTPA’s class action restriction. Opp. p. 100-102. This Court disagrees.

   a. Rule 23 Trumps Rules of Procedure

   The Rules Enabling Act, which grants the Supreme Court the power to promulgate the Federal Rules of Civil Procedure, stipulates that “[s]uch rules shall not abridge, enlarge or modify any substantive right.” 28 U.S.C. § 2072(b).

   As described above, Rule 23(a) and 23(b) list criteria for maintaining a class action suit in federal court. In Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co., the Supreme Court addressed a conflict between Rule 23 and a procedural New York State statute that precluded any claim with the ability to recover a “penalty” from proceeding as a class action. Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co., 559 U.S. 393, 397 (2010). A plurality agreed that since Rule 23 is procedural, it should trump a conflicting state procedural statute. Id. at 398. According to the plurality, the only test of a Rule’s validity under the Rules Enabling Act is “whether it regulates procedure,” and it found that Rule 23 did. Id. at 410.
Justice Stevens clarified the meaning of the plurality opinion in a concurring opinion in which he explained that Rule 23 controlled only if the conflicting state law was also procedural, and he concluded that the New York statute in question was procedural. *Id.* at 436. He held, furthermore, that Rule 23 could not supersede substantive rights created by state law, including “rules that one might describe as ‘procedural,’ but . . . nonetheless define substantive rights.” *Id.* at 425 n.8. He found that the New York law was not a substantive rule disguised as a procedural one because there were competing legislative explanations, at least one substantive and one procedural, and “[i]n order to displace a federal rule, there must be more than just a possibility that the state rule is” substantive. *Id.* at 436.

Even though the Second Circuit has yet to directly address which opinion is controlling, several other courts have concluded that Justice Stevens’s concurring opinion is controlling when analyzing class action restrictions because it was decided on the narrowest grounds. *Leonard v. Abbott Labs.*, Inc., No. 10-CV-4676(ADS)(WDW), 2012 WL 764199, at *12 (E.D.N.Y. Mar. 5, 2012) (“In contrast to the plurality opinion that categorically held that Rule 23 complied with the Rules Enabling Act, Justice Stevens agreed with the four justice dissent ‘that there are some state procedural rules that federal courts must apply in diversity cases because they function as a part of the State's definition of substantive rights and remedies.’”) (quoting *Shady Grove*, 130 S. Ct. at 1448); see also *In re Digital Music Antitrust Litig.*, 812 F. Supp. 2d 390, 415 (S.D.N.Y. 2011) (“Justice Stevens’ approach does, however, form the ‘narrowest grounds' in *Shady Grove*.”)
The five justices in the concurrence and the dissent concluded that the validity of Federal Rules of Civil Procedure turns, in part, on the rights afforded by the state rule that the Federal Rule displaces.”) (quoting In re Wellbutrin XL Antitrust Litig., 756 F. Supp. 2d 670, 675 (E.D. Pa. 2010); James River Ins. Co. v. Rapid Funding, LLC, 658 F.3d 1207, 1217 (10th Cir. 2011) (“Justice Stevens concurred, and the Tenth Circuit has understood his concurrence to be the controlling opinion in Shady Grove.”) (citing Garman v. Campbell Cnty. Sch. Dist. No. 1, 630 F.3d 977, 983 n. 6 (10th Cir. 2010)); Godin v. Schencks, 629 F.3d 79, 84 (1st Cir. 2010) (relying on Justice Stevens's concurrence in holding that “[b]ecause Section 556 is ‘so intertwined with a state right or remedy that it functions to define the scope of the state-created right,’ it cannot be displaced by Rule 12(b)(6) or Rule 56.”); In re Packaged Ice Antitrust Litig., 779 F. Supp. 2d 642, 660 (E.D. Mich. 2011) (“Courts interpreting the Shady Grove decision . . . have concluded that Justice Stevens' concurrence is the controlling opinion by which interpreting courts are bound.”); Jones v. Corr. Med. Servs., Inc., 845 F. Supp. 2d 824, 853 (W.D. Mich. 2012) (“As such, Justice Stevens's opinion should be deemed controlling here too, until the Supreme Court can further clarify the issue.”); Williams v. Chesapeake La., Inc., No. 10-1906, 2013 WL 951251, at *4 (W.D. La. March 11, 2013) (“This Court agrees that Justice Stevens reached the same result as the plurality through a narrower ground. . . . Thus, this Court will follow the standard set out in the concurrence.”); Bearden v. Honeywell Int'l, Inc., No. 09–CV–1035, 2010 WL 3239285, at *10 (M.D. Tenn. Aug. 16, 2010) (“Justice Stevens's concurrence is the controlling opinion”); Kline v. Mortg. Elec. Sec.
Sys., No. 08–CV–408, 2010 WL 6298271, at *3 (S.D. Ohio 2010) (noting that the
district courts in Ohio faced with this precise issue “have concluded
unanimously ‘that Justice Stevens' concurrence . . . is the controlling opinion by
which [they are] bound.’”) (quoting McKinney v. Bayer Corp., 744 F. Supp. 2d 733
3900716, at *6 n. 5 (D.D.C. Sept. 10, 2012) (“Justice Scalia’s opinion for the
plurality in Shady Grove controls at the ‘first step’ of the Shady Grove analysis. . .
. However, because Justice Stevens’s concurrence sets forth a narrower ground
as to the second step of the Shady Grove analysis than does Justice Scalia’s
opinion, . . . this Court agrees . . . that Justice Stevens’s concurrence controls for
that step.”). But see 3M Co. v. Butler, 842 F. Supp. 2d 85, n. 7 (D.C. Cir. 2012)
(finding that the majority opinion on the first step of the Shady Grove analysis
controls); In re OnStar Contract Litig., 2:07-MDL-01867, 2010 WL 3516691, at *4
Act’s] limitation on class actions conflicts with Rule 23 of the Federal Rules of
Civil Procedure and therefore does not prevent non-residents from pursuing
class-action claims under the MCPA in this action”). Other courts only apply the
Shady Grove analysis when the state law at issue is procedural, thereby
interpreting the majority opinion to only apply when the law at issue is procedural
not substantive. In re Frito-Lay N. Am., Inc. All Nat. Litig., No. 12-MD-
2413(RRM)(RLM), 2013 WL 4647512, at *18 (E.D.N.Y. Aug. 29, 2013) (“The
provision of New York state law at issue in Shady Grove was a procedural, not
substantive rule—like Rule 23, a precondition[] for maintaining a class action.”)
To help make sense of the fractured decision, it appears that several courts, either implicitly or explicitly, bifurcate the *Shady Grove* analysis into two steps. The first step is governed by Justice Scalia’s plurality opinion and requires a determination of whether the rule in question is procedural. If it is found to be procedural, then courts use Justice Stevens’s concurrence to analyze whether the Rule trumps the state statute at issue by determining whether the state statute is procedural or substantive. This method takes into account that five Justices, Justice Stevens and the four dissenting Justices, agreed that a Federal Rule cannot alter substantive rights under state law and disagreed with Justice Scalia’s broader holding that the Rules superseded both substantive and procedural state laws. The Court is persuaded by this synthesis.

Accordingly, the first step is to “determine whether Rule 23 answers the question in dispute,” and is, therefore, procedural. *Shady Grove Orthopedic Assocs., P.A.*, 559 U.S. at 398-399. It is clear that Rule 23 would permit a non-Connecticut resident to serve as a named plaintiff of a class action, and the Supreme Court has already determined the rule to be procedural. The next step in the analysis is determining whether CUTPA’s class action restriction is procedural or substantive. Keeping in mind that all procedural rules will have some affect on substantive rights, the Court must determine if the restriction is only procedural, and thus trumped by Rule 23, or if is substantive such that applying Rule 23 would “abridge, enlarge, or modify a [] substantive right” conferred by CUTPA, so CUTPA’s class action prohibition must be enforced. 28 U.S.C. § 2072(b).
b. CUTPA is Substantive

While the Second Circuit has yet to provide authority as to whether the restrictions in CUTPA are substantive or procedural, other courts have determined similar statutes to be substantive. For example, in *In re Wellbutrin XL Antitrust Litig.*, the court found that a restriction in the Illinois Antitrust Act (“IAA”) on actions by indirect purchasers was “intertwined with Illinois substantive rights and remedies because (1) the restrictions apply only to the IAA, (2) they are incorporated in the same statutory provision as the underlying right, not a separate procedural rule, and (3) the restrictions appear to reflect a policy judgment about managing the danger of duplicative recoveries.” *In re Wellbutrin XL Antitrust Litig.*, 756 F. Supp. 2d 670, 677 (E.D. Pa. 2010); see also *Phillips v. Philip Morris Cos. Inc.*, 290 F.R.D 476, 481 (N.D. Ohio 2013) (“The fact that [a class action restriction] is limited to actions under [Ohio’s Consumer Sales Practices Act] suggests that it was not merely intended by the state legislature to function as a procedural rule to govern class actions. Moreover, the fact that this limitation is contained within the very statute that provides consumers with an avenue for relief from unfair sales practices demonstrates that it impacts substantive rights.”).

In the case of CUTPA, the class action restriction satisfies the three *Wellbutrin* factors: (1) the class action restriction only applies to CUTPA, and nationwide class actions are still possible under other causes of action (including unjust enrichment discussed *infra*); (2) the restriction is incorporated in the same provision – and in fact in the same sentence – as that which grants the right for
residents and those injured in Connecticut to bring a class action; and (3) there is at least some evidence to suggest that the decision to restrict class actions to Connecticut residents was a purposeful policy decision.

While the first and second elements are evident from the statute itself, the third requires some examination of the statute’s legislative history. CUTPA’s prohibition states that “[p]ersons entitled to bring an action under subsection (a) of this section may . . . bring a class action on behalf of themselves and other persons similarly situated who are residents of this state or injured in this state to recover damages.” Conn. Gen. Stat. § 42-110g(b) (emphasis added). An earlier draft of CUTPA simply read: “Persons entitled to bring an action under subsection (a) of this statute may . . . bring an action on behalf of themselves and other similarly situated persons to recover damages.” H.B. 1965, 1973 Gen. Assemb., Jan. Sess. § 7(b) (Conn. 1973) (LCO No. 6719).

(the committee members did not comment on this part of her testimony). Even though the Court cannot determine the effect that this testimony had on the legislature, it is highly relevant to the present inquiry that a former draft of CUTPA did not contain the class action restriction that was ultimately added to the statute after such testimony was given. From this history, it appears that the legislature meant to restrict the amount of potential litigation to which its companies could be subject. This restriction, therefore, was not meant to be procedural, but was meant to have a substantive effect on the ability to bring a class action under CUTPA by denying that right to a subset of plaintiffs.

On the whole, this Court finds that the class action restriction in CUTPA reflects a substantive policy judgment by the Connecticut legislature. Because the restriction is substantive rather than procedural, Rule 23 cannot supersede it. Therefore, the motion to strike the CUTPA nationwide class action allegations is GRANTED.

ii. Substantive CUTPA Claim

The Trilegiant and E-Merchant Defendants also argue that (1) the Plaintiffs have not maintained a claim for a substantive CUTPA violation because they failed to plead with sufficient particularity allegations of fraud as required by Rule 9(b); and (2) that several of the CUTPA claims are barred by the relevant statute of limitations. MTD p. 33-34.
1. Pleading Sufficient Particularity

In response to the Defendant’s argument that the Plaintiffs have not pled sufficient particularity to maintain a CUTPA claim, the Plaintiffs state that they need not comply with Rule 9(b)’s heightened pleading requirements because they allege violations of CUTPA based on unfair and deceptive acts and practices in addition to their general fraud claims. Opp. 105-107. In the alternative, the Plaintiffs claim that their fraud-based allegations have the requisite particularity so as to comply with Rule 9(b). Opp. 107-109.

CUTPA provides that “[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Conn. Gen. Stat. § 42-110b(a). “[T]o prevail on a CUTPA claim, the plaintiffs must prove that (1) the defendant engaged in unfair or deceptive acts or practices in the conduct of any trade or commerce . . . and [the plaintiff suffered] ascertainable loss of money or property as a result of the defendant's acts or practices.” Neighborhood Builders, Inc. v. Town of Madison, 294 Conn. 651, 657 (2010) (quoting Conn. Gen. Stat. § 42–110b(a); Conn. Gen. Stat. § 42–110g(a)).

It is well settled that in determining whether a practice violates CUTPA we have adopted the criteria set out in the cigarette rule by the federal trade commission for determining when a practice is unfair: (1) [W]hether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise-whether, in other words, it is within at least the penumbra of some common law, statutory, or other established concept of unfairness; (2) whether it is
immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers [competitors or other businessmen].

ZeeBaaS, LLC v. Kowlewyn, No. 3:11cv11(VLB), 2012 WL 2327693, at *6 (D. Conn. June 19, 2012) (citations and internal quotation marks omitted). “All three criteria do not need to be satisfied to support a finding of unfairness. A practice may be unfair because of the degree to which it meets one of the criteria or because to a lesser extent it meets all three. . . . Thus a violation of CUTPA may be established by showing either an actual deceptive practice or a practice amounting to a violation of public policy.” Id. (citations and internal quotation marks omitted).


The Court holds that to the extent the Plaintiffs have alleged a CUTPA action based on fraud, they have failed to sufficiently plead with the particularity required in Rule 9(b) for the same reasons discussed supra. To the extent that their claims are not based on fraud, the Court must examine those claims under
the standard of Rule 8. Fed. R. Civ. P. 8(a); see CAC at ¶¶ 22, 71, 205, 206, 209, 210, 216.

The Plaintiffs allege that the Defendants violated CUTPA by engaging in “unfair and deceptive act[s] and practice[s].” CAC at ¶ 205. In supporting these claims, the Plaintiffs allege that the Trilegiant Defendants employed several business and marketing tactics in a deceptive or unfair manner with the aid of the E-Merchant Defendants and the Credit Card Defendants. CAC at ¶¶ 4-6, 8-14, 74, 117. These practices include sharing confidential billing information through datapass, employing negative option billing, and making it difficult for consumers to get refunds through the refund mitigation policy. CAC at ¶¶ 7, 81-87.

The Plaintiffs describe datapass as the transaction that occurs when confidential billing information is sent to Trilegiant to facilitate further purchases because the customer is not required to reenter credit card or debit account information. CAC at ¶¶ 7(a), 75-80. Negative option billing is the billing practice in which members are automatically charged a monthly membership fee until they affirmatively cancel their membership. CAC at ¶ 81. The Complaint fails to explain how either of these business practices are unfair or deceptive. In fact, it concedes that the negative option billing practice was disclosed in fine print on Trilegiant’s offer page. Id. Datapass, moreover, is not in and of itself an unfair practice, but like all marketing tactics can be used unfairly. Datapass can be used in a fair manner to help consumers efficiently complete several online purchases. Conversely, the Plaintiffs here have not alleged how datapass was used in an unfair or deceptive manner towards them. For example, had the
Plaintiffs alleged that datapass was used to transfer private billing information to Trilegiant who then charged for products never advertised, it may have been an unfair or deceptive use of the tool, but the Plaintiffs fail to make such allegations. By pleading only nebulous facts and inferences, the Plaintiffs have only provided conclusory allegations and have not sustained their burden on a motion to dismiss. See ZeeBaaS, LLC, 2012 WL 2327693, at *7 (conclusory allegations are insufficient to plead a CUTPA claim for unfair or deceptive practices).

The Plaintiffs have, however, made allegations sufficient to show that the refund mitigation strategy adopted by Trilegiant could have violated CUTPA. The Plaintiffs claim that call-center employees were “specifically instructed to tell customers that they somehow signed up for the Membership Programs through their credit card company,” instead of telling them the truth about their membership enrollment. CAC at ¶ 86. The Plaintiffs prove that this strategy was implemented by referencing an email in which a representative from 1-800 Flowers told a representative from Trilegiant that “we have had increasingly more frequent feedback from our own teams that your agents are telling our customers to call us” when the customer calls Trilegiant to cancel their membership. CAC at ¶ 133. Assuming these allegations to be true, call-center employees were directed to and did deceive customers calling to cancel their memberships. This misdirection would undoubtedly permit Trilegiant to charge more monthly fees while the customer attempted to discover how to cancel its membership. This claim, therefore, is actionable under CUTPA.
Accordingly, the Defendants’ motion to dismiss the individual substantive CUTPA claims is DENIED as to the refund mitigation strategy, but for all other substantive CUTPA claims it is GRANTED.

2. CUTPA Statute of Limitations

The Defendants argue that several of the Plaintiffs’ CUTPA claims are time-barred because some of the Plaintiffs enrolled in “membership programs more than three years before filing their complaints.” MTD p. 35. The Plaintiffs respond by stating that they suffered recurring injuries in the form of unauthorized monthly charges, thereby tolling the statute of limitations. Opp. p. 109. At the very least, the Plaintiffs argue that they should be able to recover for the charges that occurred within the limitations period. Id. p. 110. In the alternative, the Plaintiffs claim that the Defendants engaged in fraudulent concealment and a continuing course of conduct, both of which would toll CUTPA’s statute of limitations. Id. p. 110-14.

CUTPA is governed by a three-year statute of limitations. Conn. Gen. Stat. § 42-110g(f). It also is an occurrence statute, “meaning that the time period within which a plaintiff must commence an action begins to run at the moment the act or omission complained of occurs.” Breiner v. Stone, 122 F.3d 1055, 1055 (2d Cir. 1997) (citations and internal quotation marks omitted). CUTPA is not a discovery statute, meaning that a plaintiff does not even need to have constructive knowledge of the violation for the limitations period to run. See Argus Research Grp., Inc. v. Argus Media, Inc., 562 F. Supp. 2d 260, 279-80 (D. Conn. 2008)
(finding that CUTPA is not a discovery statute, so constructive knowledge is not relevant). It is important to note that the limitations period begins to run not from the occurrence of the injury, but from the occurrence of the alleged violation. See *Phelan ex rel. Estate of Phelan v. Daimler Chrysler Corp.*, 323 F. Supp. 2d 335, 338 (D. Conn. 2004) (“July 9 is the end point of any possible deceptive act by DCC related to inducing purchase of the jeep by Phelan’s decedent and, as such, the final date of a CUTPA violation from which the statute of limitations begins to run.”); *Johnson v. Walden Univ., Inc.*, 839 F. Supp. 2d 518, 525-26 (D. Conn. 2011) (“The acts or omissions Johnson complains of are statements made to him by his Faculty Mentor, Dr. Anderson, and representations made by Walden in its materials describing the Program, which statements and representations he alleges led him to believe he could become a practicing psychologist upon completion of the Walden Program.”).

The Plaintiffs have alleged that several of the Defendants’ business practices were unfair, deceptive, or fraudulent, and, therefore, violated CUTPA. These practices can be sorted into two groups: (1) those practices related to the alleged fraudulent enrollment into a membership program; and (2) those practices that occurred after the Plaintiffs discovered their enrollment. The first group is comprised of the sharing of confidential billing information via datapass and through the nondisclosure of the negative option billing practice. The second group is composed of the marketing or sales tactics alleged to be used in the refund mitigation strategy. The Court must determine the latest possible date of the deceptive practices and start calculating the limitation period from those
points. Assuming that the first group was not already dismissed for insufficient pleading, the first group of alleged unfair or fraudulent business practices was completed, at the latest, by the time the first or second membership fee was posted. Plaintiff Reilly alleged that the membership fee charges began shortly after May 2007; Plaintiff Restrepo alleged that the membership fee charges began on May 9, 2007; Plaintiff Warfel alleged that the membership fee charges began shortly after December 2004; and Plaintiff Williams alleged that the membership fee charges began shortly after May 26, 2009. CAC ¶¶ 27, 28, 33, 34. The first complaint for Plaintiff Reilly was dated March 2012, for Plaintiff Restrepo it was dated July 13, 2011, for Plaintiff Warfel it was dated August 4, 2011, and for Plaintiff Williams it was dated September 2012. [Dkt. 250, Defendants’ Reply Memorandum in Support of their Motion to Dismiss Plaintiffs’ Consolidated Amended Complaint or, in the Alternative, to Strike Portions of the Complaint, p. 26-27, hereinafter “Reply”]. All of these complaints were filed more than three years after the alleged violations of CUTPA from the first group of practices. Therefore, these claims would be untimely.

However, it is undisputed that the refund mitigation strategy began only after the Plaintiffs discovered the charges and called Trilegiant either to cancel their membership or to request a refund. The Plaintiffs allege that they only discovered the charges and contacted Trilegiant within three years of filing their CUTPA claims. Those claims, therefore, are timely.

The Plaintiffs ask this Court to find that the continued injury of monthly membership fees tolls the statute of limitations, or, in the alternative, that they
can recover for damages that occurred within the three year statute of limitations period. The Plaintiffs have failed, however, to allege sufficiently how charging a recurring monthly membership fee that is clearly listed on credit card statements or other banking information violates CUTPA. Moreover, these actions only constitute, at most, a repeating injury, not a recurring violation. The Plaintiffs rely on Broadway Theatre Corp. v. Buena Vista Pictures Distrib., to argue that their recurring injury should toll the statute of limitations. In Broadway Theatre Corp., the court found that the repeated issuances of exclusive distribution licenses to a movie theater created new and independent injuries because each license was a violation of CUTPA. Broadway Theatre Corp. v. Buena Vista Pictures Distrib., No. 3:00cv706(SR.), 2002 WL 32502100, at *6 (D. Conn. Sept. 19, 2002). Unlike in that case, repeated injury, in the form of recurring monthly charges, does not constitute new and independent CUTPA violations, especially when no further unfair or fraudulent activities are alleged to have occurred between the enrollment date and the discovery of the enrollment. Indeed, the court in Broadway Theater Corp. did not find that the theatre’s recurring injury would toll the statute of limitations; it found that the issuance of new distribution licenses constituted violations of CUTPA such that each issuance would have its own three year statute of limitations period. Id. Moreover, the Court held that the plaintiffs “potential damages are limited to harm suffered as a result of actions taken by the Distributors within the three-year statutory period.” Id. Following that logic, the Plaintiffs are not able to claim damages caused by CUTPA violations that occurred more than three years ago even if the harm occurred
within three years of the complaint. Since the Plaintiffs here allege that the datapass and failure to disclose the negative option billing practice occurred more than three years ago, any damages resulting from those injuries are no longer compensable.

The Plaintiffs next argue that the Defendants have engaged in fraudulent concealment, thus tolling the statute of limitations. Under the doctrine of fraudulent concealment “equitable tolling of the statute of limitations is permitted until the fraud or concealment is, or should have been, discovered by a reasonable person in the situation.” Thompson v. Accent Capital, No. 3:11CV00069(AWT), 2011 WL 3651848, at *3 (D. Conn. Aug. 18, 2011), aff’d, 491 F. App’x 264 (2d Cir. 2012) (citations and internal quotation marks omitted). Just as when analyzing the RICO claim, this Court finds that the Plaintiffs had notice of the alleged fraud when they received their credit card or debit account statements. So, no fraudulent concealment could exist past the date that the Plaintiffs received their banking information, which, based a reasonable reading of the Complaint, occurred the month after their enrollment in the Trilegiant membership programs. Furthermore, the Plaintiffs have not alleged how the Defendants concealed their fraud because submitting financial statements to the Plaintiffs actually revealed, not concealed the membership charges.

Finally, the Plaintiffs assert that the statute of limitations should be tolled under the continuing course of conduct doctrine. Even though the Connecticut Supreme Court has yet to provide clear guidance on this issue, the Court need not decide in these circumstances if the doctrine would toll the statute of

In *Phelan ex rel. Estate of Phelan v. Daimler Chrysler Corp.*, the court held that the continuing course of conduct doctrine does not apply in a vendor-vendee relationship if the plaintiff does not allege a continued pattern of deceitful conduct after the initial fraud because a vendor is under no legal obligation to disclose his initial deceitful conduct. *Phelan ex rel. Estate of Phelan*, 323 F. Supp. 2d at 339-40. Similarly here, the vendor-vendee relationship that was created between the Plaintiffs and the Defendants did not require the Defendants to disclose their initial unfair or deceptive practices. To toll the statute of limitations, the Plaintiffs need to allege a continued pattern of behavior showing that the Defendants continued to interact with the Plaintiffs in a manner perpetrating that initial fraud. *Id.* After the Plaintiffs were initially enrolled into the membership program, however, they were immediately put on notice of their enrollment and its recurring monthly fees. The Plaintiffs have not alleged that the listed charges were themselves inaccurate or fraudulent. Therefore, the Defendants did not continue in a course of conduct that concealed the existence of the alleged fraud or unfair practices, but actually acted in manner that would reveal them.
The Plaintiffs do allege, however, that when contacting Trilegiant, they experienced refund mitigation tactics, which may have resulted in a new CUTPA violation. This later fraudulent or unfair act or acts is not sufficiently tied to concealment of the initial fraud to constitute a continuing course of conduct or serve as a basis for fraudulent concealment, given that the recurring charges were repeatedly disclosed to the Plaintiffs in the form of their bank statements. Since this Court has not characterized the refund mitigation strategy as being part of the same fraudulent or unfair scheme that resulted in the membership enrollment, but rather a second potential set of CUTPA violations, the Court separates these claims for statute of limitations purposes. For that reason, damages related to the initial fraudulent inducement which occurred more than three years before the Complaint was filed would be time-barred, but those claims stemming from the potentially unfair or deceptive refund mitigation strategy tactics are timely.

For the foregoing reasons, Defendants’ motion to dismiss the CUTPA claims as to plaintiffs Reilly, Restrepo, Warfel and Williams is DENIED as to claims stemming from the refund mitigation practices, but GRANTED as to all other claims.

e. Other States’ Consumer Protection Statutes

The Defendants also move to dismiss or strike footnote 18 of the Complaint because it merely lists several other states’ consumer protection statutes without explaining how those statutes relate to the Defendants’ alleged conduct in this
In response, the Plaintiffs only allege that they are able to maintain causes of action under the various statutes in a class action proceeding, but they do not contest that they have only listed the statutes without explaining how they relate to the Defendants’ conduct. Opp. p. 104.


Here, the Plaintiffs have not incorporated any of the other state consumer protection statutes into their Complaint. Furthermore, they have not attempted to explain how the Defendants’ conduct fits into each of the undoubtedly varying elements of the statutory schemes. Without tying the Defendants’ alleged
conduct to violations of these statutes, the Plaintiffs have not sufficiently met the pleading requirements of Rule 8(a). To the extent these statutes were alleged as being alternate causes of action in the Complaint, the Defendants’ motion to dismiss is GRANTED.\(^7\) While recognizing that a party may plead in the alternative, the Court notes that claims based on desperate state statutory schemes militates against class action certification.

f. Claims for Violations of the Automatic Renewal Statute, California Business and Professional Code § 17602

The Trilegiant and E-Merchant Defendants allege that the Plaintiffs’ cause of action under the Automatic Renewal Statute must be dismissed for several reasons: (1) the Plaintiffs do not allege any facts as to how the Defendants violated the automatic renewal provision; (2) the statute only applies to offers made to consumers in California; and (3) the claims of the Plaintiffs who do reside in California are not timely because the law at issue only went into effect on December 1, 2010. MTD p. 36-37. The Plaintiffs respond that (1) they have alleged sufficient facts to show that automatic renewals were made in violation of the statute; (2) that the statute covers all consumers regardless of location; and (3) that no initial orders prior to the statute’s enactment were completed because the Plaintiffs never knowingly formed a contract with any of the Defendants related to the membership programs. The Plaintiffs have sufficiently pled a

\[^7\] Since the Defendants’ motion to dismiss was granted, the motion to strike is moot, and the Court need not decide if it is appropriate to strike that portion of the Complaint.
violation of the statute, but the statute only prohibited conduct which occurred after December 1, 2010 directed towards customers in California.

The Automatic Renewal Statute makes it unlawful for any business making an automatic renewal or continuous service offer to a consumer in this state to do any of the following: (1) Fail to present the automatic renewal offer terms or continuous service offer terms in a clear and conspicuous manner . . . (2) Charge the consumer's credit or debit card or the consumer's account with a third party for an automatic renewal or continuous service without first obtaining the consumer's affirmative consent to the agreement . . . or (3) Fail to provide an acknowledgement that includes the automatic renewal or continuous service offer terms, cancellation policy, and information regarding how to cancel . . .

Cal. Bus. & Prof. Code § 17602(a) (emphasis added). The requirements of this statute “apply only prior to the completion of the initial order for the automatic renewal or continuous service,” with limited exceptions. Id. At § 17602(d). In short, the section “prohibits a business from” “(a) failing to present the terms of the offer in a clear and conspicuous manner, (b) charging the consumer’s account without first obtaining affirmative consent, and (c) failing to provide an acknowledgment of the consumer’s enrollment in the offer.” Fields v. Wise Media, LLC, 12-cv-05160(WHA), 2013 WL 3187414, at *5 (N.D. Cal. June 21, 2013).

i. Sufficiency of Pleadings

The Plaintiffs have alleged that the Defendants were involved in enrolling and charging the Plaintiffs for membership programs without their explicit consent or knowledge. CAC at ¶¶ 77-82. They also alleged that the only
disclosure of the negative option billing practice was done in “exceedingly fine print.” CAC at ¶ 181. Accepting these allegations as true, the Plaintiffs have sufficiently pled that Trilegiant’s terms and conditions were not offered in “clear and conspicuous manner.” See id. Therefore, the Plaintiffs have sufficiently alleged facts that could constitute a violation of the Automatic Renewal Statute.

ii. Location of Injured Party

The Defendants next claim that the statute only protects individuals who were injured in California. Inexplicably the Plaintiffs disagree. Section 17602(a) states that it “shall be unlawful for any business making an automatic renewal or continuous service offer to a consumer in this state,” meaning California. The only other court to have had occasion to address this issue found that the text of the statute clearly creates a cause of action only for consumers that are residents of or were harmed in California. See Noll v. eBay Inc., 11-cv-0485(EJD), 2013 WL 2384250, at *6 (N.D. Cal. May 30, 2013) (finding that the Automatic Renewal Statute provided a private right of action only for California residents). In Noll v. eBay Inc., the court found that the statute’s plain language prohibited a Florida resident from bringing a claim for relief. Id. It noted that in other provisions in the same code, the legislature created causes of action for out-of-state customers, but chose not to include that right in this statute. Id. The court refused to “contravene the Legislature’s clear intention” to limit the cause of action in this statute. Id.
We agree that the Automatic Renewal Statute only provides a private cause of action for customers who are harmed in California. Any holding to the contrary would clearly abrogate the statute’s plain text and could have serious constitutional implications. See Reply. p. 21, n.17. Therefore, the claims arising under the Automatic Renewal Statute from the Plaintiffs who were harmed outside of California are DISMISSED.

iii. Date of Injury

The Defendants claim that the statute only protects consumers who were harmed after December 1, 2010. MTD p. 36. The Plaintiffs argue that they were harmed after December 1, 2010 because they did not consent to an “initial order” prior to that date. Opp. p. 128-30. Furthermore, they assert that the recurring credit card or debit account charges after December 1, 2010 cause the claims to be actionable. Id.

The California legislature stated that “[t]his article shall become operative on December 1, 2010.” 2009 Cal. Leg Serv. Ch. 350 (S.B. 340) (WEST) § 1; Cal. Bus. & Prof. Code § 17606. The default rule of statutory construction is that statutes apply prospectively unless the legislature has manifested a clear intent to the contrary. See Landgraf v. USI Film Prods., 511 U.S. 244, 274 (1994) (“But while the constitutional impediments to retroactive civil legislation are now modest, prospectivity remains the appropriate default rule.”) (emphasis in the original). Here, the legislature manifested its intent for the statute’s prospective application by explicitly setting its operative date without limitation or exception.
Therefore, for an injury to be cognizable under the statute, the violation must have occurred on and after December 1, 2010 because before this date, the statute was inactive. Moreover, the Plaintiffs do not argue that the statute should apply retroactively.

Instead, the Plaintiffs argue that the violation occurred after December 1, 2010 because they failed to read their monthly statements and were therefore unaware that they were paying recurring monthly membership fees for Trilegiant’s membership programs until they actually read their statements and discovered the recurring monthly charges. The Plaintiffs’ argument that they had no “initial order” as required by the statute because they did not consent to forming the initial contract is unavailing because they would no longer have standing to bring a cause of action under this statute. Section 17602(d) states that a company must disclose the terms and conditions of the renewal obligation before “completion of the initial order.” Cal. Bus. & Policy Code § 17602(d). This means that to violate the statute, companies must fail to disclose the automatic renewal practice before the first order is completed. Therefore, if the Plaintiffs have not completed any “initial orders,” the companies have not breached any obligations.

Contrary to both the Plaintiffs’ and Defendants’ arguments, section 17602(d) has no bearing on when the statute became effective; it only dictates when the companies offering the automatic renewal must comply with the statute’s requirements. After the initial order is complete, the company is not required to continue making the necessary disclosures except as provided by the
statute. Considering the statute’s affirmative obligations, to state a cause of action under this statute, a plaintiff must allege that he or she was enrolled in a membership program without being adequately notified of the automatic renewal provision after December 1, 2010. Since all of the Plaintiffs allege becoming Trilegiant members before that date, the claims under this statute are not cognizable. CAC at ¶¶ 24-34.

The Plaintiffs’ argument that their continued injury in the form of monthly membership dues tolled the statute of limitations for this action is inapplicable. Because the statute was not in effect at the time the alleged violation occurred, there was no cause of action to toll. Further, because the Court views the Plaintiffs as having no cause of action under the Automatic Renewal Statute, it does not decide whether continued injury tolls the relevant statute of limitations.

Defendants’ motion to dismiss the Automatic Renewal Statute claims is GRANTED.

g. **Claims for Unjust Enrichment**

The Defendants move to dismiss the Plaintiffs’ unjust enrichment claim because the Plaintiffs have not “plausibly pleaded any conduct that is ‘fraudulent, deceptive [or] wrongful,’” and because “the CAC does not allege that Plaintiffs conferred any benefit on any Defendant except the Trilegiant Defendants.” MTD p. 37-38. The Plaintiffs reply that they have pled with sufficient detail the unjust nature of the Defendants’ actions and have alleged how each group of
Defendants has received some benefit from the unjust, fraudulent, or otherwise wrongful conduct. Opp. p. 130-132.

Under Connecticut law, unjust enrichment is a “broad and flexible remedy,” and plaintiffs seeking recovery under this theory “must prove (1) that the defendants were benefited, (2) that the defendants unjustly did not pay the plaintiffs for the benefits, and (3) that the failure of payment was to the plaintiffs’ detriment.” Vertex, Inc. v. City of Waterbury, 278 Conn. 557, 573 (Conn. 2006) (citations and internal quotation marks omitted). “This doctrine is based upon the principle that one should not be permitted unjustly to enrich himself at the expense of another but should be required to make restitution of or for property received, retained or appropriated . . . . The question is: Did [the party liable], to the detriment of someone else, obtain something of value to which [the party liable] was not entitled?” Town of New Hartford v. Conn. Res. Recovery Auth., 291 Conn. 433, 451 (Conn. 2009) (citations and internal quotation marks omitted).

Under the liberal construction of the pleadings doctrine at the motion to dismiss stage, the Court finds that the Plaintiffs have sufficiently pled their unjust enrichment claim as to the Trilegiant and E-Merchant Defendants.

The alleged fraudulent, deceptive, or unfair business practices of the Defendants have been discussed at length, and do not require much repetition here. In short, the Plaintiffs have alleged that the Defendants tricked them into enrolling into a membership program, and then would automatically charge them recurring membership fees; when the Plaintiffs finally discovered that they were
being charged, the Defendants would make it incredibly difficult for them to obtain a refund. CAC at ¶¶ 24-35, 71-82. As part of the refund mitigation strategy, the E-Merchant Defendants were heavily involved in organizing and implementing the tactics. CAC at ¶¶ 8, 133. The Plaintiffs further allege that as part of this process, Trilegiant paid the E-Merchant Defendants signing bonuses and “sizeable percentage[s]” of each dollar collected from the E-Merchant’s customers. CAC at ¶¶ 5, 6, 104, 119-133. These allegations are sufficient under Rule 8(a) to sustain a claim for unjust enrichment against the Trilegiant and E-Merchant Defendants. See Keaney v. Eastern Computer Exch., Inc., No. 03-cv-1893(RNC), 2004 WL 885100, at *2 (D. Conn. April 21, 2004) (allegations in a complaint are liberally construed on a motion to dismiss, “all plaintiff need allege is that the individual defendants have benefited from his services to Eastern, and unjustly failed to pay him for the benefits, to his detriment.”); see also Jewell v. The Med. Protective Co., No. 03-cv-1157(RNC), 2003 WL 22682332, at *2 (D. Conn. Oct. 30, 2003).

However, the Plaintiffs have failed to allege sufficiently how the Credit Card Defendants were involved in the scheme or were unjustly enriched. Indeed, the Plaintiffs admitted that “Trilegiant and Affinion conduct legitimate business of selling the Membership Programs through lawful means.” CAC at ¶ 154. They then accuse the Credit Card Defendants of furthering the scheme by not refusing to process Trilegiant membership charges. The Plaintiffs fail to allege, however, how the Credit Card Defendants could have known what members were willing participants in Trilegiant’s membership programs and which members felt that
they were fraudulently enrolled. The Plaintiffs’ conclusory allegations that the numerous Credit Card Defendants knew that the charges were fraudulent because they had some type of unidentified anti-fraud program and they collectively received thousands of complaints by Trilegiant customers, without any indication of the order of magnitude of the complaints, are not sufficient.

Moreover, the Plaintiffs’ conclusion that the Credit Card Defendants reviewed Trilegiant call-center scripts and participated in calls with customers seeking a refund does nothing more than explain that the Credit Card Defendants were taking their customer complaints seriously. CAC at ¶ 11(b). Furthermore, unlike the E-Merchant Defendants who received substantial bounties directly tied to every dollar that Trilegiant made, the Plaintiffs only allege that the Credit Card Defendants engaged in the ordinary course of business by processing charges at their standard processing fee rate for all of their customers, including Trilegiant. CAC at ¶ 12. The Credit Card Defendants also never allegedly engaged in any acts to conceal the fraud as they were the Defendants who sent the Plaintiffs financial statements clearly indicating the membership charges. CAC at ¶ 160(h). On these facts and conclusions alone, the Plaintiffs have not sufficiently shown how the Credit Card Defendants were involved in the alleged unjust behavior or how they were unjustly enriched.

For the foregoing reasons, the Defendants’ motion to dismiss the Plaintiffs’ unjust enrichment claims is DENIED as to the Trilegiant and E-Merchant Defendants and GRANTED as to the Credit Card Defendants.
h. The Pederson Class Action Settlement

The Defendants argue that Plaintiffs Reilly, Restrepo, Brian Schnabel, and Warfel should be barred from bringing claims against the Defendants because they were included in a prior class action settlement in which they specifically released all claims against the Defendants for the activity alleged in this Complaint. MTD p. 38-42. The Plaintiffs respond by stating that they were not included in the prior class because their injuries extended outside of the prior class’s temporal definition. Opp. 134. The Court disagrees with the Plaintiffs and finds that the Plaintiffs are barred from bringing their current claims because of the prior class action settlement.

At the outset, a court may “judicially notice prior pleadings, orders, judgments, and other items appearing in the court records of prior litigation that are related to the case before the Court.” Patrowicz v. Transamerica HomeFirst, Inc., 359 F. Supp. 2d 140, 144-145 (D. Conn. 2005); see also Steinmetz v. Toyota Motor Credit Corp., 963 F. Supp. 1294, 1298-99 (E.D.N.Y. 1997) (judicial proceedings from state courts, including prior class action settlement agreements will have binding res judicata effect under the full faith and credit clause). The Plaintiffs do not contest that the Court may take judicial notice of the Pederson Settlement Agreement or contest the binding nature of that prior agreement.

The definition of the Settlement Class in the Pederson litigation is incredibly broad, and includes “[a]ll persons and entities who had unsolicited or
unauthorized charges for Trilegiant products posted to their credit card, debit card, phone, bank, mortgage, or other billing accounts by Trilegiant or a Marketing Partner and who paid Trilegiant for those products at any time from July 10, 1998, until February 15, 2008.” See Exhibit 4 to MTD, Pederson v. Trilegiant, No. 01-L-1126 (Ill. Cir. Ct. July 18, 2008). The Plaintiffs contend that they are not members of this class because they were charged monthly fees after February 15, 2008. This definition, however, clearly encompasses all people who had unsolicited or unauthorized charges prior to February 15, 2008 regardless of what happened after that date. In the Complaint, Plaintiffs Reilly, Restrepo, Brian Schnabel, and Warfel all admitted that they had unauthorized charges for a Trilegiant membership program prior to February 15, 2008. Accordingly, they are by definition class members in the Pederson proceeding.

The Class members agreed to release all claims against Trilegiant and other “released persons,” which includes the E-Marketing Defendants and the Credit Card Defendants here, arising from “the marketing, sale and/or purchase of a Product or the provision of a Product by the released Persons, whether known or unknown, suspected or unsuspected, asserted or unasserted, foreseen or unforeseen, actual or contingent, liquidated or unliquidated . . . .” Id. at ¶ 12.

The Plaintiffs do not allege, nor could they, that the matters at issue in this Complaint are not barred by the prior settlement. Since the Plaintiffs named above are members of that former class, their claims must be dismissed.
The Plaintiffs hint at, but fail to argue, a possibly compelling due process argument related to the notice that the Pederson class members received or, more appropriately, failed to receive. *See Hecht v. United Collection Bureau, Inc.*, 691 F.3d 218, 221-26 (2d Cir. 2012) (reversing the district court's dismissal of a claim based on res judicata due to a settlement agreement because notice in one national newspaper did not comport was due process protections). Unfortunately, the Plaintiffs only state that “there is simply no evidentiary basis at this early stage” to conclude that they were given proper notice. Opp. p. 134, n.80. Even if they did not receive proper notice, the Court posits without deciding that it would appear that such a challenge should be brought before the court in which the class action settlement was approved.

The Defendants’ motion to dismiss the claims of Plaintiffs Reilly, Restrepo, Brian Schnabel, and Warfel as being barred by the prior settlement agreement is GRANTED.

i. **Motion to Strike the Allegations Regarding Previous Investigations and Attorneys General Settlements**

The Defendants move to strike the Plaintiffs’ allegations regarding the Senate Report and settlements between the Trilegiant Defendants and state attorneys general because these allegations are immaterial to the case at hand. MTD, p. 42, 43. The Defendants argue that since the Plaintiffs are only using these past reports and agreements to prove further the Defendants’ liability in the present matter or to show liability in prior proceedings, the allegations violate the federal rules of evidence, and, therefore, will be inadmissible at trial. *Id.* The
Plaintiffs respond by stating that they are not using the Senate Report or the settlement agreements to prove liability in the present matter, but for other purposes permitted under the federal rules of evidence, such as to prove the Defendants’ knowledge, motive, or notice. Opp. p. 136. These allegations are immaterial to the present proceeding and have no purpose remaining in the Complaint.

In “deciding whether to strike a Rule 12(f) motion on the ground that the matter is impertinent and immaterial, it is settled that the motion will be denied, unless it can be shown that no evidence in support of the allegation would be admissible.” *Lipsky v. Commonwealth United Corp.*, 551 F.2d 887, 892-94 (2d Cir. 1976). “Evidentiary questions, such as the one present in this case, should especially be avoided at such a preliminary stage of the proceedings. . . . And ordinarily neither a district court nor an appellate court should decide to strike a portion of the complaint on the grounds that the material could not possibly be relevant on the sterile field of the pleadings alone.” *Id.* (citing *Gleason v. Chain Service Restaurant*, 300 F. Supp. 1241 (S.D.N.Y. 1969), aff’d, 422 F.2d 342 (2d Cir. 1970)); *Fleischer v. A. A. P., Inc.*, 180 F. Supp. 717 (S.D.N.Y. 1959); 2A Moore’s Federal Practice P 12-21(1) (2d ed. 1975)). Nevertheless, “Second Circuit case law makes clear that references to preliminary steps in litigations and administrative proceedings that did not result in an adjudication on the merits or legal or permissible findings of fact are, as a matter of law, immaterial under Rule 12(f) of the Federal Rules of Civil Procedure” in cases where they are being used “as substantive evidence of previous wrongdoing” or to prove liability. *In re Merrill*
Lynch & Co., Inc. Research Reports Securities Litig., 218 F.R.D. 76, 78 (S.D.N.Y. 2003); Dent v. U.S. Tennis Ass’n, Inc., No. 08-cv-1533, 2008 WL 2483288, at *2 (E.D.N.Y. June 17, 2008); In re Platinum & Palladium Commodities Litig., 828 F. Supp. 2d 588, 594 (S.D.N.Y. 2011 ) (stating that plaintiffs were prohibited from relying on a CFTC order to plead the “underlying facts of liability” because it “was the product of a settlement between the CFTC and the Respondents, not an adjudication of the underlying issues in the CFTC proceeding.”) (quoting United States v. Gilbert, 668 F.2d 94, 97 (2d Cir. 1981)).

Initially, it is unclear to the Court how the prior settlement with the attorneys general is relevant to the present matter. In that case, the resolution, as the Plaintiffs describe it, was that “Trilegiant was enjoined from directly marketing its Membership Programs through mail solicitations without making certain changes to its practice.” CAC at ¶ 6 (emphasis added). The Plaintiffs also admitted that after that settlement, Trilegiant “mutated its business practices into their current form.” CAC at ¶ 17 (emphasis added). Furthermore, only Trilegiant and Chase were parties to those prior settlements. Clearly, the Plaintiffs are not attempting to show that the past conduct is the same conduct at issue in this case. Therefore, this Court does not find the discussion of those prior settlements as material to the present Complaint.

On the other hand, the Senate Report seems to discuss nearly identical commercial behavior that the Plaintiffs allege gives rise to their causes of action here. The Report concluded “that the E-Merchant Defendants engaged in deceptive conduct and violated credit card company rules by automatically
transferring customer’s credit card information to Trilegiant.” CAC at ¶ 16. However, the Plaintiffs do not provide much detail explaining why the Senate reached this conclusion. Even so, it appears that the investigation’s conclusions were not derived from the adversarial process, but from a one-sided factual inquiry. While these reports are important for future legislation, they should have no bearing on a Defendant’s liability before a Court of law. Moreover, the excerpts that the Plaintiffs provide in the pleadings do not define Trilegiant’s marketing or banking partners. So, it does not appear that the Plaintiffs intend to use the report to show knowledge or notice. The only purpose that the Court can draw from the inclusion of these allegations in the Complaint is to show proof of the Defendants’ liability either for past activities of prior bad acts or for activities identical to the claims alleged here.

Since the purpose of the pleadings is to put the Defendants on notice as to how they violated the necessary elements of the causes of action stated by the Plaintiffs and because facts related to unadjudicated investigations or settlements are not permitted to prove liability, the Senate Report and the settlement by the states’ attorneys general are immaterial and impertinent to the present action. If they are to be used at trial, the Plaintiffs may present the evidence later and the Defendants will have an opportunity to object to their admissibility. However, as a matter of pleading, the allegations do not further the Plaintiffs’ stated causes of action, and should be stricken from the pleadings.

For the foregoing reasons, the Defendants’ motion to strike is GRANTED.
V. Conclusion

For the foregoing reasons, the Defendants’ [Dkt. 189] Motion to Dismiss Plaintiffs’ Consolidated Amended Class Action Complaint or, in the Alternative, to Strike Portions of the Complaint is GRANTED IN PART and DENIED IN PART:

- The Plaintiffs’ substantive RICO claims against all Defendants are DISMISSED;
- The Plaintiff’s conspiracy to violate RICO claims against all Defendants are DISMISSED;
- The Plaintiffs’ claims for violations of the California Automatic Renewal Statute against the Trilegiant and E-Merchant Defendants are DISMISSED;
- The claims by Plaintiffs Reilly, Restrepo, Brian Schnabel, and Warfel against all Defendants are DISMISSED;
- The Defendants’ motion to strike the Plaintiffs’ CUTPA class action allegations is GRANTED;
- The Defendants’ motion to Dismiss footnote 18 of the Complaint is GRANTED;
- The Defendants’ motion to strike references to the Senate Report and prior settlement with the states’ attorneys general is GRANTED.

However, a few claims remain extant:

- The Defendants’ motion to dismiss the Plaintiffs’ claims for CUTPA violations stemming from the refund mitigation strategy against the Trilegiant and E-Merchant Defendants is DENIED, but as to all other alleged CUTPA violations it is GRANTED;
- The Defendants’ motion to dismiss the Plaintiffs’ claims for unjust enrichment against the Trilegiant and E-Merchant Defendants is DENIED, but the motion to dismiss claims for unjust enrichment against the Credit Card Defendants is GRANTED;
The Defendants’ motion to dismiss the Plaintiffs’ ECPA claims against Trilegiant, Affinion, and the E-Merchant Defendants brought by Plaintiffs Kelm, Pham, Reilly, Restrepo, Brian Schnabel, Warfel, and Williams is GRANTED, but the Defendants’ motion to dismiss the ECPA claims against Trilegiant, Affinion, and the E-Merchant Defendants brought by Plaintiffs DiCarolis, Edward and Lucy Schnabel, Sumlin, and Timmcke is DENIED.

IT IS SO ORDERED.


______________________________
/s/
Hon. Vanessa L. Bryant
United States District Judge

Dated at Hartford, Connecticut: March 28, 2014
INTRODUCTION

In this putative class action, viewers of Hulu’s on-line video content allege that Hulu wrongfully disclosed their video viewing selections and personal identification information to third parties such as metrics companies (meaning, companies that track data) and social networks, in violation of the Video Privacy Protection Act (“VPPA”), 18 U.S.C. § 2710. Second Amended Consolidated Class Action Complaint (“SAC”), ECF No. 83 at 7-8. In their class certification motion, Plaintiffs limit the third parties to comScore, a metrics company that analyzes Hulu’s viewing audience and provides reports that Hulu uses to get media content and sell advertising, and the social network Facebook. See Motion For Class Certification, ECF No. 111.

The Act prohibits a “video tape service provider” from knowingly disclosing “personally

1 Citations are to the Electronic Case File (“ECF”) with pin cites to the electronic page number at the top of the document.
identifiable information of a consumer of the provider’” to third parties except under identified exceptions that do not apply here. See 18 U.S.C. § 2710. “The term ‘personally identifiable information’ includes information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” Id. § 2710(a)(3).

Hulu argues that it did not violate the VPPA because (I) it disclosed only anonymous user IDs and never linked the user IDs to identifying data such as a person’s name or address; (II) it did not disclose the information “knowingly” and thus is not liable; and (III) Hulu users who are Facebook users consented to the disclosures because Facebook’s terms of use permitted disclosure. Motion for Summary Judgment, ECF No. 125-4 at 1-2.

The court grants the summary judgment motion as to the comScore disclosures and denies it as to the Facebook disclosures. The comScore disclosures were anonymous disclosures that hypothetically could have been linked to video watching. That is not enough to establish a VPPA violation. As to the Facebook disclosures, there are material issues of fact about whether the disclosure of the video name was tied to an identified Facebook user such that it was a prohibited disclosure under the VPPA. In addition, the record is not developed enough for the court to determine as a matter of law whether Hulu knowingly disclosed information or whether Hulu users consented to the disclosures.

STATEMENT

I. THE PARTIES AND THE PROPOSED CLASSES

Hulu provides on-demand, online access to television shows, movies, and other pre-recorded video content from networks and studios through its website, www.hulu.com. SAC ¶¶ 1, 17. It offers a free service at hulu.com that allows users to watch video content on their computers. See Joint Statement of Undisputed Facts (“JSUF”) #1. It also offers a paid service called “Hulu Plus” that has more content and allows viewers to watch Hulu content on other devices such as tablets and smart phones. Yang Decl. ¶¶ 2, 6.

Plaintiffs Joseph Garvey, Sandra Peralta, Paul Torre, Joshua Wymyczak, and Evan Zampella each are registered Hulu users. See SAC ¶¶ 1-6. Sandra Peralta, Evan Zampella, and Paul Torre became paying Hulu Plus subscribers in July 2010, June 2011, and July 2012, respectively. See id.
¶ 3-4, 6, 34. The SAC alleges that Hulu wrongfully disclosed Plaintiffs’ video viewing selections and “personally identifiable information” to third parties comScore and Facebook, all in violation of the VPPA.  See id. ¶¶ 51-63; Motion for Class Certification, ECF No. 111.

Plaintiffs ask the court to certify two classes: the comScore disclosure class and the Facebook disclosure class.  See Class Cert. Motion, ECF No. 111 at 2.  The class definition are as follows:

**comScore Disclosure Class**

All persons residing in the United States and its territories who, from March 4, 2011 through November 8, 2012, were registered users of hulu.com (including, but not limited to, paying subscribers, also known as Hulu Plus subscribers) and requested and/or obtained video materials and/or services on hulu.com during the Class Period.

**Facebook Disclosure Class**

All persons residing in the United States and its territories who, from April 21, 2010 through June 7, 2012, were registered users of hulu.com (including, but not limited to, paying subscribers, also known as Hulu Plus subscribers) and requested and/or obtained video materials and/or services on hulu.com during the Class Period.

**II. HOW HULU WORKS**

Hulu pays license fees to studios, networks, and other rights holders to obtain the video content that it offers to its users.  See Yang Decl, ¶ 10, ECF No. 12-6.  Hulu allows users to register for a free Hulu account.  See JSUF #1.  A Hulu user does not need to register for a Hulu account to watch videos on hulu.com using a personal computer.  See Yang Decl. ¶ 4.  To register for a Hulu account, the user enters a first and last name, birth date, gender, and an email address.  JSUF #1.  Users are not required to provide their legal first and last name during registration.  JSUF #2.  In fact, Plaintiff Joseph Garvey registered for his Hulu account in a name other than his legal name.  See JSUF #3.  Hulu does not verify the accuracy of the identifying information but stores it in a secure location.  Yang Decl. ¶ 6.  To register for Hulu Plus, the user must provide the same information as a registered Hulu user, payment information, and a billing address.  Yang Decl. ¶ 7.  Hulu assigned each new registered Hulu user a “User ID,” which is a unique numerical identifier of at least seven digits (e.g., 50253776). JSUF #6; see Tom Dep., Carpenter Decl. Ex. 7, ECF No. 157-11 at 37:9-38:12.

The videos on hulu.com are displayed on a video player that appears on a webpage.  Hulu calls these webpages “watch pages.”  See Yang Decl. ¶ 3; see JSUF #24.  Hulu wrote and deployed the
code for its watch pages. Tom Dep., Carpenter Decl. Ex. 7, ECF No. 157-11, at 108:23-109:8, 175:9-16; Wu Dep., Carpenter Decl. Ex. 2, ECF No. 157-6, at 80-84. The code downloaded to registered Hulu users’ browsers when they visited a watch page so that the browser could display the requested web page or video content. Tom Depo., Carpenter Decl. Ex. 7, ECF No. 157-11 at 112:19-113:5. As described in more detail below, the code also allowed information to be transmitted to comScore and Facebook. Until June 7, 2012, the URL (uniform resource locator, meaning, the web address) of Hulu’s watch pages included the name of the video on that page (e.g., http://www.hulu.com/watch/426520/saturday-night-live-the-californians-thanksgiving). JSUF #24 (the number in the URL, here 426520, is the video ID).

On or about March 12, 2009, Hulu began providing each registered user with a profile web page. JSUF #9. The first and last name the user provided during registration appears on the page and in the page title. JSUF #10. Hulu did not allow registered users to decline to share their first and last names on their public profile pages. Until August 1, 2011, a user’s profile page URL included the user’s unencrypted Hulu User ID. JSUF #12. An example is http://www.hulu.com/profiles/u/[UserID], where “[UserID]” is the Hulu User ID. Id. After August 1, 2011, the Hulu User ID was encrypted. JSUF #13. An example is http://www.hulu.com/profiles/u/wxu2RqZLhrBtVjYKEC_R4. Id. Hulu did not provide a separate search function (for example, through a search box) to allow a user to use a Hulu User ID to find the profile page of another user. JSUF #11. On May 30, 2013, Hulu discontinued the user profile pages. JSUF #14.

Hulu makes money from advertising revenue and from monthly premiums paid by Hulu Plus members. Yang Decl., ¶ 11. Its main source of income is advertising revenue. Id. Advertisers pay Hulu to run commercials at periodic breaks during video playback. Id. ¶ 12. Advertisers pay based on how many times an ad is viewed. Id. ¶ 13. Hulu thus gathers information (or metrics) about its “audience size.” Id. Advertisers require verified metrics, which means that Hulu needs to hire trusted metrics companies. Id. comScore is one of those companies. Id. ¶ 14.

Hulu-comScore contract). As of 2013, comScore captured 1.5 trillion digital interactions each month and had more than 2000 clients. *Id.* Ex. 22; see *Harris v. comScore, Inc.*, 292 F.R.D. 579, 581 (N.D. Ill. 2013) (describing comScore’s business).

### III. HOW HULU INTERACTS WITH COMSCORE

According to Hulu, comScore gives it “reports containing metrics regarding the size of the audience for programming on hulu.com,” and Hulu uses the reports to obtain programming and sell advertising. Yang Decl., ECF No. 125-6, ¶ 14. The reports never identify a user by name and instead present the data in an “aggregated and generalized basis, without reference even to User IDs.” *Id.* Hulu uses the comScore metrics to show “other content owners . . . that the Hulu audience is a desirable outlet for their programming, and to convince advertisers of the value of reaching Hulu’s audience.” *Id.* Mr. Yang said in his deposition that he did not know why Hulu sent individual comScore user IDs (see below) if comScore provided only aggregate information, and he did not know whether comScore provided other reports with individual-level data. See Yang Dep., ECF No. 125-3 at 102-04, 108-11.

comScore uses “beacon” technology to track audience metrics. *Id.* ¶ 15. A “beacon” is triggered by defined events during the playing of a video such as when the video starts, when the advertisement starts, when it ends, and when the video re-starts. *Id.* The beacon, when triggered by an event, directs the user’s browser to send a piece of HTTP programming code to comScore that contains certain defined “parameters” (meaning, pieces of data or information). *Id.* ¶ 16.

From March 27, 2010 through November 8, 2012, when a user watched a video on hulu.com, Hulu, which wrote the code to transmit the data, transmitted information to comScore by using a comScore “beacon” on the Hulu watch page. JSUF #4-5. The beacon included four pieces of information: (1) the Hulu user’s unique numerical Hulu User ID; (2) the “GUID,” a long alphanumeric string that Hulu used to differentiate between web browsers and that Hulu assigned at random to a browser when it accessed hulu.com; (3) the Hulu “Ad ID,” a unique six-digit number that identifies only the advertisement; and (4) the name of the program and any season or episode.

---

2  An example of a “GUID” is 767DE299767B4E577B787B40B5123C30. JSUF #7.

comScore’s possession of the Hulu User ID allowed it to connect all information that was tied to
that Hulu User ID. See Calandrino Decl., ECF No. 160-5, ¶¶ 30, 33-34, 47. Because the Hulu User
ID was in the URL of users’ profile page, comScore had the “key” to locating users’ associated
profiles that revealed the names the users provided when they signed up for Hulu. Id. ¶¶ 35-37. The
user profile pages were all in a standard format: http://www.hulu.com/profiles/u/[User ID]. As
discussed above, the watch page contained the video title. The argument is that comScore could
easily access the profile page and see the user’s first and last names (or at least the names that the
users gave when registering) and connect that to the user’s viewing information. For Hulu Plus
members, presumably the names would correspond to their billing and payment information (and
thus likely reflected the users’ true names).

The code Hulu wrote and included in each watch page also caused a unique numeric or
alphanumeric “comScore UID” for each registered user to be communicated from the registered
user’s browser to comScore. See Wills Decl., ECF No. 160-6, ¶¶ 36-37; JSUF#15, 17. The
comScore UID is stored in a comScore cookie and identifies the specific copy of the web browser.
JSUF #15-17. The comScore cookie enabled comScore to link the identified user and video choice
information to other information it gained about the same user when the user visited websites where
comScore collects data. Calandrino Decl., ECF No. 160-5, ¶¶ 48-56; Wills Decl. ECF No. 160-6,
¶ 36.

For context, a cookie is a file on a user’s computer. Wu Decl., ECF No. 125-7, ¶ 13. Cookies
contain information that identifies the domain name of the webserver that wrote the cookie (e.g.,
hulu.com, comScore.com, or facebook.com). Id. ¶ 18. Cookies have information about the user’s
interaction with a website. Id. Examples include how the website should be displayed, how many
times a user has visited the website, what pages he visited, and authentication information. Id. ¶ 13.

Each web browser on a computer (e.g., Internet Explorer or Chrome) stores the cookies that are
created during a user’s use of the browser in a folder on the user’s computer that is unique to that
browser. Id. ¶ 14. When a user types a website address into the browser, the browser sends (a) a
request to load the page to the webserver for that website address and (b) any cookies that are
associated with the website (such as the cookies on the user’s computer for “hulu.com” or “comScore.com”). *Id.* ¶ 15. The remote website server returns the requested page and can update the cookies or write new ones. *Id.* The only servers that can access a particular cookie are those associated with the domain that wrote the cookie. *Id.* ¶¶ 18, 21. That means that Hulu can read only hulu.com cookies, and it cannot read comScore.com cookies or facebook.com cookies.

That being said, according to Plaintiffs, Hulu hosts its vendors’ JavaScript code on Hulu’s domain so that when Hulu’s web pages execute the vendor code, a vendor such as comScore obtains information through cookies that are set by hulu.com. *See* Carpenter Decl. Ex. 10, ECF No. 158-2 at HULU_GAR231508 (vendors need to set cookies on hulu.com for tracking; example given was google analytics); *id.* Ex 11, ECF No. 158-3 at HULU_GAR 093686 (email from Hulu to Google; hulu user goes to hulu.com to watch a video; user’s browser calls invite_media (presumably where content is); cookies from there will be passed on to Google; Google can set cookies on the user). More specifically as to comScore, Hulu’s documents have examples of code that sets comScore identifiers, including its UID and UIDR cookies. *See id.* Exs. 11-15, ECF Nos. 158-3 to 158-7.

**IV. HOW HULU INTERACTS WITH FACEBOOK**

Facebook collects information and processes content “shared by its users,” and it provides that information to marketers when it sells them its products (identified as “Facebook Ads,” “Facebook Ad System,” and “Ad Analytics and Facebook Insights”). *See* Carpenter Decl. Ex. 8, ECF No. 157-12 (Facebook 2012 SEC Form 10-K). Facebook shares its members’ information with marketers so that marketers can target their ad campaigns. *See id.* Marketers can “specify the types of users they want to reach based on information that users choose to share.” *Id.* Advertisement revenue is how Facebook makes money. *See id.*

Certain information was transmitted from hulu.com to Facebook via the Facebook “Like” button through June 7, 2012 (when Hulu stopped including the video title in the watch page URL). JSUF #18. During this time period, Hulu included a Facebook Like button on each hulu.com watch page. JSUF #18-19. Hulu wrote code for its watch pages that included code for where the “Like” button should be located on the page and where (from facebook.com) to obtain the code that loads and operates the button. JSUF #20. When the user’s browser executed this code, the browser sent the
request to Facebook to load the Like button. JSUF #21. The request included a “referer URL” value (the URL of the page from which the request issued) in the request headers and the query string. JSUF #21. That is how Facebook knows where to send code for the Like button so that it can be downloaded and used. Wu Decl. ¶¶ 16, 20. Until June 7, 2012, the URL for each watch page included the title of the video displayed on that watch page. See JSUF #18. The IP address of the Hulu registered user’s computer also was sent to Facebook (although there are scenarios when the IP address might not be that of the users but instead of a proxy or intermediary). See Tom Depo., Carpenter Decl. Ex. 7, ECF No. 157-11 at 190:23-192:12.

Facebook also received the following cookies associated with the facebook.com domain: (1) a “datr” cookie, which identifies the browser; (2) a “lu” cookie, which “can contain the Facebook user ID [e.g., 286xxxx1] of the previous Facebook user to log in to Facebook via the browser and has a lifetime of ‘two years’;” and (3) if the user had logged into Facebook using default settings within the previous four weeks, a “c_user” cookie, which contains the logged-in user’s Facebook user ID. JSUF #22; Calandrino Decl. ¶ 71. Hulu did not send Facebook the Hulu User ID or the Hulu user’s name when the user’s browser executed the code to load the Like button. JSUF #23.

No evidence has been introduced that Facebook took any actions with the cookies described above. JSUF #25. That being said, Plaintiffs’ expert opines that Hulu’s disclosure to Facebook of cookie identifiers set by Facebook’s domain enabled Facebook to link information identifying the user and the user’s video choices to other information about the particular user. See Calandrino Decl., ECF No. 160-5, ¶¶ 57-81. In common web browsers, visiting a website out of Facebook’s control will not result in the communication of information to Facebook absent a decision (directly or indirectly) by the party controlling the website to send information. Id. ¶ 57. It is straightforward to develop a web page that “yields no communication with Facebook.” Id. When a Hulu watch page loaded with the Facebook Like button, the page prompted a user’s web browser to transmit the watch page URL and Facebook cookies to Facebook-controlled servers. Id. ¶ 58. This happened with the initial Hulu-prompted request from the user’s browser to Facebook before the receipt of any information from Facebook. Id. ¶ 59. Because the URL of the watch page specified the title of the video during the period from April 21, 2010 to June 7, 2012, Facebook would know the title of the
video being viewed. *Id.* ¶ 61. The c_user cookie would give the name of the currently-logged in Facebook user. *Id.* ¶ 66. The lu cookie might too. *Id.* ¶ 71. A user is logged out of Facebook by default after closing the browser, but Facebook also provides users with an option to remain logged in after closing the browser. *Id.* ¶¶ 72-73. The lu cookie clears after a user selects Facebook’s log-out option. *Id.* ¶ 74.

**ANALYSIS**

**I. SUMMARY JUDGMENT**

The court must grant a motion for summary judgment if the movant shows that there is no genuine dispute as to any material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986). Material facts are those that may affect the outcome of the case. *Anderson*, 477 U.S. at 248. A dispute about a material fact is genuine if there is sufficient evidence for a reasonable jury to return a verdict for the non-moving party. *Id.* at 248-49.

The party moving for summary judgment has the initial burden of informing the court of the basis for the motion and identifying those portions of the pleadings, depositions, answers to interrogatories, admissions, or affidavits that demonstrate the absence of a triable issue of material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). To meet its burden, “the moving party must either produce evidence negating an essential element of the nonmoving party’s claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial.” *Nissan Fire & Marine Ins. Co., Ltd. v. Fritz Companies, Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000); see *Devereaux v. Abbey*, 263 F.3d 1070, 1076 (9th Cir. 2001) (“When the nonmoving party has the burden of proof at trial, the moving party need only point out ‘that there is an absence of evidence to support the nonmoving party’s case.’”) (quoting *Celotex*, 477 U.S. at 325).

If the moving party meets its initial burden, the burden shifts to the non-moving party, which must go beyond the pleadings and submit admissible evidence supporting its claims or defenses and showing a genuine issue for trial. See Fed. R. Civ. P. 56(e); *Celotex*, 477 U.S. at 324; *Nissan Fire*, 210 F.3d at 1103; *Devereaux*, 263 F.3d at 1076. If the non-moving party does not produce evidence
to show a genuine issue of material fact, the moving party is entitled to summary judgment. *See Celotex*, 477 U.S. at 323.


**II. THE VIDEO PRIVACY PROTECTION ACT AND DISCLOSURES OF USER IDS**


“Aggrieved” persons may sue for knowing disclosures of information in violation of the statute. *See* 18 U.S.C. § 2710(b)-(c). Under the statute, a “court may award – (A) actual damages but not less than liquidated damages in an amount of $2,500; (B) punitive damages; (C) reasonable attorneys’ fees and other litigation costs reasonably incurred; and (D) such other preliminary and equitable relief as the court determines to be appropriate.” 28 U.S.C. §§ 2710(c)(2).

Plaintiffs purport to represent a class of “aggrieved persons.” As consumers of Hulu’s video content, they sue Hulu for transmitting their identifying information and the videos they watched to comScore and Facebook. The issue is whether the information transmitted to comScore and Facebook is “information which identifies a person as having requested or obtained specific video materials.” 18 U.S.C. § 2710(a)(3). If it is, then the transmission violates the VPPA. *See id.* & 2710(b).

The next part of this order has three sections: A, B, and C. Section A analyzes the plain language of the statute and the legislative history and concludes that disclosed information must identify a specific person and tie that person to video content that the person watched in order to violate the VPPA. Section B examines whether there are triable issues of fact about whether the information transmitted to comScore and Facebook identified the watcher specifically enough to
establish a violation of the VPPA. Section B also addresses Hulu’s argument that any disclosures were not “knowing.” Section C addresses Hulu’s argument that Facebook users consented to the disclosures.

A. The VPPA Prohibits Disclosures That Ties Specific People to the Videos They Watch

The VPPA prohibits a “videotape service provider” from (1) knowingly disclosing “to any person” (2) “personally identifiable information” concerning any “consumer” of such provider. See 18 U.S.C. § 2710(b) (emphasis added to identify terms to be defined).

A “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710 (a)(4). The court previously held that Hulu was a “video tape service provider” within the meaning of the act. See 8/10/12 Order, ECF No. 68 at 7-9.

A “consumer” is “any renter, purchaser, or subscriber of goods or services from a video tape service provider.” 28 U.S.C. § 2710(a)(1). The court previously held that Plaintiffs were consumers within the meaning of the Act. See 8/10/12 Order, ECF No. 68 at 11-12.

“The term ‘personally identifiable information’ [“PII”] includes information which identifies a person as having requested or obtained specific video materials or services.” Id. § 2710(a)(3).

The VPPA allows certain disclosures including the following: (1) disclosures to the consumer; (2) disclosures to any person with the informed, written consent of the consumer given at the time the disclosure is sought;3 (3) disclosures to law enforcement; or (4) disclosures that are “incident to the ordinary course of business,” defined as “debt collection activities, order fulfillment, request processing, and the transfer of ownership.” 28 U.S.C. § 2710(a)(2) & (b)(2). The transmissions here are not incident to Hulu’s “ordinary course of business” as that term is defined in the statute. See 8/10/12 Order, ECF No. 68 at 9-10. For example, as discussed below, Hulu initiated the transmission of the Facebook ID cookies before any action by Facebook, and the cookies were not necessary to Hulu’s order fulfillment and request processing. Tracking start-stop times for

---

advertising might require identification of an anonymized user ID, but the comScore UID was not
part of orders processing. Indeed, the point of the ID cookies was to track Hulu users’ activities.
The other exceptions do not apply.

The issue is whether Hulu’s disclosures here (unique numeric identifications tied to video
watching) are PII under the VPPA. The statute’s plain language prohibits disclosure of information
that “identifies a person” as having (in the Hulu context) viewed specific video content. 28 U.S.C.
§ 2710(a)(3). It does not say “identify by name” and thus plainly encompasses other means of
identifying a person. Indeed, PII is not given one definition: “the term . . . includes information
which identifies a person. . . .” Id. That being said, considering the ordinary meaning of the plain
language of the statute, the language supports the conclusion that the disclosure must be pegged to
an identifiable person (as opposed to an anonymous person). The statute’s plain language is
ambiguous about whether it covers unique anonymous user IDs such as the Hulu ID. The court thus
turns to the legislative history.

Congress’s impetus for passing the VPPA was a newspaper’s obtaining a list of video tapes that
Supreme Court nominee and D.C. Circuit Judge Robert Bork rented from his local video store and
then publishing an article about his viewing preferences. See Dikes, 936 F. Supp. at 238 (citing S.
Rep. 100-599, 2d Sess. at 5). The Senate Report shows the legislature’s concern with disclosures
linked to particular, identified individuals. It states that VPPA’s purpose was “[t]o preserve personal
privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual

It is nobody’s business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch
on television or read . . . . In an era of interactive television cables, the growth of computer
checking and check-out counters, of security systems and telephones, all lodged together in
computers, it would be relatively easy at some point to give a profile of a person and tell
what they buy in a store, what kind of food they like, what sort of television programs they
watch. . . . I think that is wrong, I think that really is Big Brother, and I think it is something
that we have to guard against.

Id. at *5-6. Senator Leahy also expressed concern about sophisticated information-tracking:

[The trail of information generated by every transaction that is now recorded and stored in
sophisticated record-keeping systems is a new, more subtle and pervasive form of
surveillance. These ‘information pools’ create privacy interests that directly affect the ability
of people to express their opinions, to join in association with others and to enjoy the
freedom and independence that the Constitution was established to safeguard.
The bill prohibits video stores from disclosing “personally identifiable information” – information that links the customer or patron to particular materials or services. In the event of an unauthorized disclosure, an individual may bring a civil action for damages.

Id. at *7. The Senate Report includes an section-by-section analysis of the VPPA that elaborates on the statutory definition of personally-identifiable information:

The term “personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape services provider. Unlike the other definitions in this subsection, paragraph (a)(3) uses the word ‘includes’ to establish a minimum, but not exclusive, definition of personally identifiable information.

... This definition makes clear that personally identifiable information is intended to be transaction-oriented. It is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider. The bill does not restrict the disclosure of information other than personally identifiable information. Thus, for example, a video tape service provider is not prohibited from responding to a law enforcement agent’s inquiry as to whether a person patronized a video tape service provider at a particular time or on a particular date.

See id. at *11-12.

The plain language of the statute suggests, and the Senate Report confirms, that the statute protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched. See id. at *7.

B. The Disclosures to comScore and Facebook

The issue then is whether the disclosures here are merely an anonymized ID or whether they are closer to linking identified persons to the videos they watched. A summary of the alleged disclosures is as follows:

1. Disclosure to comScore of Watch Page and Hulu User ID. The disclosure to comScore is of a “watch page” URL web address containing the video name and the Hulu user’s unique seven-digit Hulu User ID. The ID also appeared in unencrypted form in the URL web address for the user’s profile page in the standard format http://www.hulu.com/profiles/u/[User ID]. The profile page also listed the user’s name (or at least the first and last name used to register with Hulu). This meant that comScore could access the profile page and see the user’s first and last names.
2. Disclosure to comScore of the comScore UID (User ID) Cookie. Hulu sent comScore a “comScore ID” that was unique to each registered user. This allowed comScore to link the identified user and the user’s video choices with information that comScore gathered from other websites that the same user visited. See Calandrino Decl. ¶¶ 48-56, ECF No. 160-5; Wills Decl. ¶ 36, ECF No. 160-6 at 10.

3. Disclosure to Facebook of Watch Page and Transmission of Facebook Cookies to Facebook. These disclosures included unique identifiers that sometimes included the user’s IP address and sometimes contained the user’s Facebook ID. Because the URL web address had the video name, Facebook could see its users and what they were watching.

Hulu argues that it is not liable for these three disclosures because it never combined or linked the user IDs to identifying data such as a person’s name or address. Motion, ECF No. 125-4 at 7. It characterizes Plaintiffs’ comScore case as “the theoretical possibility that comScore could have used the anonymous ID . . . to find the user’s name.” Id. at 8. It characterizes the Facebook case as “plaintiffs’ evidence does not show that Facebook was gathering the actual name of its users from Hulu pages” and “there is no evidence that Facebook ever linked the anonymized identifier to a person’s name, or to the title of a video that person watched.” It concludes that the disclosure of the information here (even if linked to a specific video) is not a violation of the VPPA.

No case has addressed directly the issues raised by Plaintiffs: the disclosure of their unique identifiers and the videos they are watching. Most cases involve identified customers linked to the videos they watch. See, e.g., Amazon.com LLC v. Lay, 758 F. Supp. 2d 1154, 1159 (W.D. Wash. 2010) (specific customer purchasers); Mollett v. Netflix, No. 5:11-CV-01629-EJD, 2012 WL 3731542 (N.D. Cal. Aug. 17, 2012) (Plaintiffs were viewers who watched Netflix videos through a “Netflix Ready Device” such as a game console, DVD player, or Internet television; Netflix’s procedures required only a one-time password during the initial set-up; family members could see what Plaintiffs had watched; no VPPA violation because the disclosure was to consumers who thereafter were responsible for limiting access to their devices). Few cases even address unique anonymous IDs.

Hulu cites it for the proposition that a unique, anonymous ID is not identifying information under the VPPA. Motion ECF No. 125-4 at 17. The case involved a discovery dispute in a copyright case brought by Viacom against YouTube. *Viacom*, 253 F.R.D. at 262. Viacom wanted YouTube’s “logging” database that contained, “for each instance a video is watched, the unique ‘login ID’ of the user who watched it, the time when the user started to watch the video, the internet protocol address for other devices connected to the internet use to identify the user’s computer . . . , and the identifier for the video.” *Id.* at 261. YouTube argued that the VPPA barred it from disclosing the information. *Id.* at 262. What was at issue, however, was not the users’ identities. Instead, because the case was a copyright case against YouTube, what mattered was the number of times the users viewed particular videos. *Id.* YouTube “did not refute that the login ID is an anonymous pseudonym that users create for themselves when they sign up with YouTube which without more cannot identify specific individuals.” *Id.* at 262 (emphasis added). The court dismissed YouTube’s privacy concerns as speculative and ordered discovery. *Id.*

That result makes sense: the case was about discovery to establish copyright damages, not consumers’ identities. The consumer identities were not relevant. Indeed, Viacom issued a press release that the parties would anonymize the data before disclosure to address YouTube users’ privacy concerns. *See* Carpenter Decl. Ex. 21, ECF No. 156-21. Also, the decision does not provide enough of a factual context to determine whether the user IDs in *Viacom* identified a person or were anonymized. The case’s holding is relevant only to the extent that it recognizes that unique anonymous IDs do not necessarily identify people.

Another case that addressed unique anonymous IDs was *Lahr v. NTSB*, a Freedom of Information Act (“FOIA”) case. *See* 453 F. Supp. 2d 1153, 1183 (C.D. Cal. 2006), *rev’d in part on other grounds*, 569 F.3d 969 (9th Cir. 2009). The *Lahr* court held that witness identification numbers alone did not disclose private information or allow access to the witnesses. *See id.* The FOIA applicant challenged the government’s refusal to produce records relating to the investigation of an airplane that exploded in mid-air. The court applied the balancing test under the applicable FOIA exemption and held that the public interest in disclosure outweighed the government’s objection that disclosing witness identification numbers would harm the witnesses’ “interest in not
being subjected to unofficial questioning . . . and in avoiding annoyance or harassment in their . . .
private lives.” Id. at 1177, 1183-84. That holding was grounded on the government’s “fail[ure] to
explain how the disclosure of witness identification numbers, alone, could provide access to these
individuals or any personally identifying information about them. Furthermore, the identification
numbers are not personal information of a nature ordinarily protected by the courts under [the FOIA
exemption], such as social security numbers or personnel records.” Id. at 1183. Again, this decision
supports only the conclusion that personally-identifiable information requires more than a unique
anonymous ID.

Hulu cites a third unpublished case from the 10th Circuit that addresses the scope of PII under
the Cable Act. See Pruitt v. Comcast Cable Holdings, LLC, 100 F. App’x 713, 716 (10th Cir. 2004).
The Cable Act is a 1984 Act that establishes a scheme for the protection of personally-identifiable
information regarding cable subscribers. See 47 U.S.C. § 551. Courts hold that the VPPA is
analogous to the Cable Act. See Parker v. Time Warner Entm’t Co., No. 98 CV 4265(ERK), 1999
WL 1132463, at *9 (E.D.N.Y. Nov. 8, 1999). Like the VPPA, the Cable Act prohibits disclosure to
third parties. The issue in Pruitt was whether Comcast disclosed PII by issuing the appellants’ old
cable converter boxes to new customers without deleting the pay-per-view purchase histories stored
in the cable boxes. 1999 WL 1132463, at *9. The court held that it did not because the converter
boxes did not contain “the name, address or any information regarding the customer.” Id. Instead,
they contained a hexadecimal code that “enables Comcast to identify a customer’s viewing habits by
connecting the coded information with its billing management system.” Id. The district court noted
that “the converter box code – without more – provides nothing but a series of numbers.” Id. The
Tenth Circuit agreed, explaining:

Without the information in the billing or management system one cannot connect the unit
address with a specific customer; without the billing information, even Comcast would be
unable to identify which individual household was associated with the raw data in the
converter box. Consequently, it is the billing system that holds the key to obtaining
personally identifiable information, not the converter box.

Pruitt, 100 F. App’x at 716. Pruitt stands for the proposition that an anonymous, unique ID without
more does not constitute PII. But it also suggests that if an anonymous, unique ID were disclosed to
a person who could understand it, that might constitute PII.
Hulu nonetheless argues that the disclosure has to be the person’s actual name. Motion, ECF No. 125-4 at 18. That position paints too bright a line. One could not skirt liability under the VPPA, for example, by disclosing a unique identifier and a correlated look-up table. The statute does not require a name. It defines PII as a term that “includes information which identifies a person.” 18 U.S.C. § 2710(a)(3). The legislative history shows Congress used the word “includes” when it defined PII to establish a minimum, but not exclusive, definition. See S. Rep. 100-599, at *11-12. It is information that “identifies a particular person as having engaged in a specific transaction with a video tape service provider” by retaining or obtaining specific video materials or services. Id. at *12; 18 U.S.C. § 2710(a)(3). It does not require identification by a name necessarily. One can be identified in many ways: by a picture, by pointing, by an employee number, by the station or office or cubicle where one works, by telling someone what “that person” rented.

In sum, the statute, the legislative history, and the case law do not require a name, instead require the identification of a specific person tied to a specific transaction, and support the conclusion that a unique anonymized ID alone is not PII but context could render it not anonymous and the equivalent of the identification of a specific person.

Hulu’s other cited cases do not change this result. For example, it cites Low v. LinkedIn Corp. for the proposition that transmitting anonymous cookies is not a transmission of private information merely because the receiving party could “de-anonymize” the plaintiff’s identity. See 900 F. Supp. 2d 1010 (N.D. Cal. 2012). The Low plaintiffs sued LinkedIn for transmitting their browsing histories (including their LinkedIn user IDs) to advertising and marketing companies. See 900 F. Supp. 2d at 1016-18. The privacy interest arose under the California Constitution, which requires a legally-protected privacy interest, a reasonable expectation of privacy under the circumstances, and conduct that amounts to a serious invasion of the protected interest. Id. at 1023. The court noted that the transmission of code was not the “‘serious invasion’ of a protected property interest” that the Constitution protected. Id. at 1024. The case does not alter the conclusion that a unique anonymized ID could be PII if other evidence renders it the equivalent of identifying a specific person.

Hulu’s other cases similarly support only the conclusion that anonymous identification data
alone is not PII. See, e.g., Millennium TGA, Inc. v. Comcast Cable Commc’ns, LLC, 286 F.R.D. 8, 15-16 (D.D.C. 2012) (Comcast’s disclosure of city and state information for subscribers that Plaintiff identified by IP address was not PII); Steinberg v. CVS Caremark Corp., 899 F. Supp. 2d 331, 335-37 (E.D. Pa. 2012) (dismissed class action alleging disclosure of HIPPA-protected patient information for failure to state a claim; defendant sold “de-identified” prescription information to vendors who potentially could “re-identify” the information; no evidence that they had done so; proof would have been expert testimony about the risk of re-identification).

Plaintiffs argue that someone who possesses a unique identifier for an individual “requires no further information to distinguish the individual from the rest of the population.” Opposition, ECF No. 155 at 9 (quoting Calandrino Decl. ¶ 28). But the issue is whether a unique identifier – without more – violates the VPPA. It does not. The VPPA prohibits the disclosure of a particular person’s viewing choices to “any person,” meaning, a third party. See 18 U.S.C. § 2710(b). The VPPA requires identifying the viewers and their video choices.

Plaintiffs also analogize to 16 C.F.R. § 312, the FTC’s rule that defines personal information under the Children’s Online Protection Act broadly to include persistent identifiers in cookies or online information that is combined with an identifier. Opposition, ECF No. 155 at 10. Protection of children online implicates different privacy concerns and resulted in broader definitions of personal information. By contrast, the VPPA prohibits only disclosure of a particular viewer’s watched videos.

The next sections apply this analysis to the three disclosures, which differ in the information disclosed about a Hulu user and what happened with the disclosure.

1. Disclosure to comScore of Watch Page and Hulu User IDs

Hulu’s liability here is based on the hypothetical that comScore could use the Hulu ID to access the Hulu user’s profile page to obtain the user’s name. Hulu characterizes this argument as “reverse engineering” its data. The idea is that comScore could capture the data from the watch page, extract the relevant information (the video name and Hulu User ID), and plug the data into the standard-format URL for the profile page to capture the user’s name from that page. There is no evidence that comScore did this. The issue is only that it could.
At summary judgment, Hulu carried its initial burden by pointing to the absence of information that comScore correlated any information such that there is a disclosure within the meaning of the VPPA: “information which identifies a person as having requested or obtained specific video materials or services.” See 18 U.S.C. § 2710(a)(3). Plaintiffs did not point to any evidence showing genuine disputes on any material fact about whether comScore did anything with the information. The evidence shows comScore’s role in measuring whether users watched the advertisements. It also demonstrates comScore’s interest in recognizing users and tracking their visits to other websites where comScore collects data. That information likely is relevant to an advertiser’s desire to target ads to them. It does not suggest any linking of a specific, identified person and his video habits. The court grants summary judgment in Hulu’s favor on this theory.²

2. The comScore UID (User ID) Cookie

For similar reasons, the court grants Hulu summary judgment on this theory. The disclosure is that Hulu coded the hulu.com watch pages to cause the user’s web browser to send comScore a “comScore ID” that was unique to each registered user. These unique cookies allow comScore to recognize users and track their visits to other websites where comScore collects data. The point of the cookies is to recognize users to collect data about them, and here, that data included video choices. See Opposition, ECF No. 155 at 17-19; Calandrino Decl. ¶¶ 48-56, ECF No. 160-5; Wills Decl. ¶ 36, ECF No. 160-6 at 10. Looking at the evidence very practically, comScore doubtless collects as much evidence as it can about what webpages Hulu users visit. Its cookies help it do that. There may be substantial tracking that reveals a lot of information about a person. The cookies may show someone’s consumption relevant to an advertiser’s desire to target ads to them. And there is a VPPA violation only if that tracking necessarily reveals an identified person and his video watching. There is no genuine issue of material fact that the tracking here did that. The fact that Hulu wrote the code that sent the cookie does not alter this conclusion.

⁴ comScore submitted a declaration in support of Hulu’s opposition to Plaintiffs’ class certification motion saying that it did not use any information it collected from hulu.com to personally identify any of Hulu’s users or to link their PII to their requested or watched videos on hulu.com. See Johnson Decl., ECF No. 143, ¶ 12. The court does not rely on that declaration here.
3. Disclosure to Facebook of Watch Page and Transmission of Facebook Cookies to Facebook.

Hulu sent code and information to load the Facebook Like button that included the following: (1) the watch page with the video name; (2) generally the user’s IP address; (2) the datr cookie identifying the browser; (3) the lu cookie that identified the previous Facebook user using the browser to log into Facebook (with a life of two years); and (4) the c_user cookie for any user who logged into Facebook using the default setting in the past four weeks. At the summary judgment stage, it is not clear to the court whether the datr cookie alone establishes a VPPA violation because it apparently reveals only the browser, and it is not clear that it is the linking of the specific, identified person to his watched videos that is necessary for a VPPA violation. See Calandrino Decl., ECF No. 160-5, ¶78. But the lu and the c_user cookies – sent with the datr cookie at the same time the watch page loaded with the video name – together reveal information about what the Hulu user watched and who the Hulu user is on Facebook. It also is a Hulu-initiated transmission of information.

Hulu argues that it never sent the “actual” name of any Facebook user. See Motion, ECF No. 125-4 at 22. Instead, the name came from the user’s web browser and the interaction that Facebook had with its users. Id. It argues that this data transfer is based on standard Internet processes, without Hulu’s involvement.” Id. at 12. The “standard Internet process” is described above in the section of the Statement on cookies. See supra Statement, “III. How Hulu Interacts with comScore” (describing cookies). The user types a website address into the browser (e.g., www.facebook.com), and the browser sends a request to load the page along with the remote website’s cookies that are already stored on the user’s computer (here, the lu and c_user cookies). See Wu Decl., ECF No. 125-7, ¶ 15.

The Hulu-Facebook interaction here was a Hulu-prompted request from the Hulu user’s browser

---

5 According to a declaration filed in support of Plaintiffs’ motion for class certification, the Facebook datr cookie value uniquely corresponds to a particular Facebook user, whether or not the user is logged into Facebook, and it can track the user’s activity on Facebook and on other websites and associate it to the user’s Facebook profile information. See Wills Decl., ECF No. 160-6, ¶ 42a. Despite that declaration, it apparently identifies only the browser.
to Facebook to load the Like button (as opposed to a user’s request to load a Facebook page or a
Hulu user’s clicking on the Like button) that occurred before Facebook sent any data or instructions
or cookies.  *Id.* ¶ 59. According to Plaintiffs, Hulu wrote the code that sent the lu and c_user
cookies stored on the Hulu user’s computer that had information about the Hulu user’s actual
identity on Facebook. This is not merely the transmission of a unique, anonymous ID; it is
information that identifies the Hulu user’s actual identity on Facebook. The transmission was not
the Hulu/Facebook user’s decision. Instead, it was done automatically using Hulu’s code to load the
Facebook Like button. It may be true – as Hulu says – that accessing a remote browser involves
sending that browser’s cookies. But according to Plaintiffs’ expert, it was straightforward to
develop a webpage that would not communicate information to Facebook. *Id.* ¶ 57. Put another
way, it was not necessary to send the “Facebook user” cookies, and they were sent because Hulu
chose to include the Like button on watch pages.

Those Facebook ID cookies (the lu and c_user cookies) were transmitted with the watch page
and the embedded video name. Thus, the process was an electronic transmission of the Hulu user’s
actual identity on Facebook and the video that the Facebook user was watching. *See* Calandrino
Decl. ¶¶ 67-69 (the cookies transmitted the user’s Facebook ID). Depending on Hulu’s knowledge,
that could be a VPPA violation. The analysis would be different if the Facebook cookies were sent
when a user pressed the Like button. Information transmitted as a necessary part of a user’s decision
to share his views about his videos with his friends on Facebook would not support a VPPA
violation.

Hulu argues that it needed to send an actual name to be liable and that it sent only cookies.
Motion, ECF No. 125-4 at 22-23. The statute does not require an actual name and requires only
something akin to it. If the cookies contained a Facebook ID, they could show the Hulu user’s
identity on Facebook. According to Plaintiffs’ expert, “persons registered on Facebook must
provide their real names when creating Facebook accounts.” *Wills Decl.* ¶ 50. More to the point, a
Facebook user – even one using a nickname – generally is an identified person on a social network
platform. The Facebook User ID is more than a unique, anonymous identifier. It personally
identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion.
Code is a language, and languages contain names, and the string is the Facebook user name. There is a material issue of fact that the information transmitted to Facebook was sufficient to identify individual consumers. See Calandrino Decl., ECF No. 160-5, ¶ 68-69, 79-81.

Hulu also argues that the data sent to Facebook is not necessarily PII because it reveals only the last Facebook user to log in to that computer or use that browser. Reply Brief, ECF No. 140 at 8-9 (citing Calandrino Decl. ¶ 66). That may be so for devices with multiple users. It also is a fact issue. Again assuming Hulu’s knowledge, there could be VPPA violations for users who were the only users of their devices or browsers. Also, Plaintiffs limit their statutory damages to one VPPA violation.

Hulu also argues that there is no evidence that Facebook took any actions with the cookies after receiving them. JSUF #25. It also says that there is no evidence that Facebook tied its Facebook user cookies to the URL for the watch page (and the accompanying title). Motion, ECF No. 125-4 at 15, 24. In contrast to comScore, where the user was not tied to the video in one transmission, the transmission to Facebook included the video name and Facebook user cookies. Thus, the link between user and video was more obvious. But Hulu’s point is that the information really was not disclosed to Facebook in the sense that the information about Judge Bork’s video viewing was disclosed to the Washington Post.

Whether this link was the equivalent of a disclosure under the VPPA depends on the facts. One can think of analogies in a paper world. Throwing Judge Bork’s video watch list in the recycle bin is not a disclosure. Throwing it in the bin knowing that the Washington Post searches your bin every evening for intelligence about local luminaries might be. The issue is whether Hulu made a “knowing” disclosure.

The statute requires a “knowing” disclosure “to any person.” See 18 U.S.C. § 2710(b)(1). The emphasis is on disclosure, not comprehension by the receiving person. See S. Rep. 100-599, at *12 (“[s]ection 2710(b)(1) establishes a statutory presumption that the disclosure of personally identifiable information is a violation” unless a statutory exception applies). Thus, the Seventh Circuit held that the practice of placing PII on parking tickets in the view of the public was a disclosure that violated the analogous Driver’s Privacy Protection Act, regardless of whether anyone
viewed the PII. See Senne v. Village of Palatine Ill., 695 F.3d 597 (7th Cir. 2012) (en banc). By analogy, if a video store knowingly hands a list of Judge Bork’s rented videos to a Washington Post reporter, it arguably violates the VPPA even if the reporter does not look at the list.

Still, disclosure of information on traffic tickets in public view or providing a list of videos is different than transmission of cookies tied to a watch page. The first disclosures transmit obvious PII. The second transmits cookies with identifying information that is the equivalent of a name only to someone who has the ability to read it. Moreover, the VPPA prohibits a knowing disclosure to “any person,” and the point of that prohibition is to prevent disclosure of a person’s video viewing preferences to someone else.

No case has construed the word “knowingly” as it appears in the VPPA. Other cases involving violations of privacy statutes show that in the context of a disclosure of private information, “knowingly” means consciousness of transmitting the private information. It does not mean merely transmitting the code. See Freedman v. America Online, Inc., 329 F. Supp. 2d 745, 748-89 (E.D. Va. 2004) (faxing subscriber information to a police officer was knowingly divulging information protected by the Electronic Communication Privacy Act, 18 U.S.C. § 2701); Muskovich v. Crowell, No. 08 C 50015, 1996 WL 707008 (S.D. Iowa Aug. 30, 1996) (MCI employee obtained customer’s private phone number from records; MCI’s failure to implement adequate security procedures was not a knowing divulgement of her information).

Here, considering the statute’s reach, the conclusion is that Hulu’s transmission of the Facebook user cookies needs to be the equivalent of knowingly identifying a specific person as “having requested or obtained specific video materials or services.” See 18 U.S.C. § 2710(a)(3). If Hulu did not know that it was transmitting both an identifier and the person’s video watching information, then there is no violation of the VPPA. By contrast, if it did know what it was transmitting, then (depending on the facts) there might be a VPPA violation.

The issue then is what do the undisputed facts show about what Hulu knew. Hulu points to the parties’ joint undisputed fact that “[n]o evidence has been introduced that Facebook took any actions with the [datr, lu, and c_user] cookies . . . after receiving them.” JSUF #25. That the parties did not introduce evidence does not obviously end the inquiry. On the one hand, Facebook did receive the
packets of information (specific user information and videos watched) together. That is different
than the comScore disclosures, which required comScore to tie information together in non-obvious
ways. On the other hand, the Facebook user cookies are more like the Comcast hexidecimal
customer codes that could identify a customer in Pruitt. The court’s view is that if Hulu never knew
that Facebook might “read” the videos and the Facebook ID cookies together in a manner akin to the
disclosure of Judge Bork’s videos, then there is not a VPPA violation. The problem here is that the
JSUF shows only that there is no evidence “introduced” on whether Facebook took any actions with
the Facebook ID cookies. That is not the same as saying, “there is no evidence at all.” For example,
it might be dispositive if Facebook could not auto-authenticate a user when the Like button loaded.

Hulu’s next argument is that the cookies are “unintelligible” and “owned by Facebook[, and, a]s
a result, Hulu cannot access that cookie or read information stored in it” and “could not have known
what data Facebook was receiving. Accordingly, even if Facebook was collecting identifying
information, Hulu did not ‘knowingly’ disclose that information to Facebook.” Motion, ECF No.
125-4 at 17. Hulu’s only evidentiary support for this argument is the following paragraph:

The domain value for cookies means that the only servers which can access browser cookies are
the servers associated with the domains that wrote the cookies. Therefore, a webserver
associated with hulu.com will only access cookies with the domain hulu.com and a webserver
associated with facebook.com will only access cookies with the domain facebook.com.

Wu Decl., ECF No. 125-7, ¶ 21.

This description – that only servers associated with the domain that writes a cookie can access
that domain’s cookie – does not answer the question about what Hulu knew. Instead, it only
describes how servers can read cookies. Hulu may not have been able to read Facebook’s cookies,
but if it knew what they contained and knew that it was transmitting PII – that is, information that
“identifies a person as having requested or obtained specific video materials or services,” 18 U.S.C.
§ 2710(a)(3) – then Hulu is liable under the VPPA.

In sum, arguing that transmitting cookies is just the normal way that webpages and the Like
button load is not enough to negate knowledge or show the absence of evidence about knowledge.
See Celotex, 477 U.S. at 325. Thus, the burden does not shift to Plaintiffs to submit admissible
evidence showing a genuine issue for trial. That being said, there is additional information that
suggests fact issues about Hulu’s knowledge.

The transmission of the cookies to load the Like button was not necessary to Hulu’s business and instead apparently was a benefit for Facebook to leverage its platform and gain information about its users (presumably through the deployment of the Like Button). (The same is true of the comScore UID, which allowed comScore to track and gain information about users.) Hulu wrote and installed the code that integrated the Like button on the watch pages, and it transmitted the Facebook ID cookies when it sent the request to Facebook to load the Like button. See supra; Wu Decl., ECF No. 125-7, ¶ 25.

Emails about cookie placement establish that Hulu knew that vendors can place cookies on the user’s computer. See, e.g., Carpenter Decl. Ex. 11. Emails also show Hulu knew that cookies with identifying information were sent, Hulu’s awareness that vendors could collect data and use it for other purposes to build a profile or “identify a user in the real world,” and Hulu’s recognition of the VPPA implications. See Carpenter Decl. Ex. 1; id. Ex. 5, HULU_GAR 177541 (noting VPPA implications); id. Ex. 9, HULU_GAR 19274 (concern with sending video titles to eHarmony).

Another email states, “there are concerns around using beacons that send user data, along with the referrer ID, on a user-identifiable basis. Even with contractual restrictions, we can’t rule out the possibility that someone might object to these practices for these or other reasons. But I said that Hulu had made the judgment that it would accept that legal risk given the business benefits of these analytics.” See id., Ex. 5, HULU_GAR 164822; see id. at HULU_GAR 164825 (Hulu made the judgment to accept the risk of passing identifying data “so long as it is not passing unique, identifying information, which sounds like you might be doing here . . . .”).

These points suggest purposefulness about allowing the use of vendor cookies to track Hulu users. They also suggest that Hulu knew that using beacon technology to disclose user data could result in identification of actual users, and it recognized the VPPA implications. And again, Hulu wrote and installed the code that integrated the Like button on the watch pages, and it transmitted the Facebook ID cookies when it sent the request to Facebook to load the Like button.

With comScore, again, the purposefulness of cookie use was less consequential given (a) the steps that comScore would need to take to tie the video to an identified user and (b) the reality of
comScore’s business model. That is why there are no issues of material fact as to comScore. With Facebook, the cookies are transmitted when the watch page with the video name loads, and the point of the transmission is to load the Like button. The process of loading the Like button was not the decision of the Facebook/Hulu user, and instead, Hulu wrote the code that transmitted identifying information without that user’s permission. If Hulu and Facebook negotiated the exchange of cookies so that Facebook could track information (including watched videos) about its users on Hulu’s platform when the Like button loaded, or if Hulu knew that it was transmitting Facebook ID cookies and video watch pages, then there might be a VPPA violation. The record shows fact issues about Hulu’s knowledge.

Another reason to deny summary judgment on this record is that this was an early summary judgment motion before the close of discovery. Plaintiffs are reviewing documents and source code still, and the motion was filed before this review and the class certification hearing. See Opposition, ECF No. 155 at 6. The court cannot dispose of a case involving fact questions about knowledge on an undeveloped record with a half-page argument about knowledge at the end of a brief that mostly is directed to Hulu’s main argument that the alphanumeric strings here are not unique identifiers equivalent to a name.

The court denies Hulu’s summary judgment motion regarding the disclosures to Facebook.

C. Whether Facebook Users Consented to the “Like” Button’s Function

The VPPA permits disclosure to any consumer with the consumer’s informed, written consent. During the class period, the VPPA’s consent provisions – later amended effective January 2013 – required “the informed, written consent of the consumer given at the time the disclosure is sought.” 18 U.S.C. § 2710(b)(2)(B). Hulu cites only Facebook’s current policies and information on its Help Center in September 2013. Motion, ECF No. 125-4 at 24-25. There is no evidence about the policies in place during the class period of April 21, 2010 to June 7, 2012. If the 2013 Facebook policies were in place then (and it seems doubtful), Hulu did not say so. Also, Hulu does not explain why Facebook’s data policies are the equivalent of the VPPA’s “informed, written consent at the time of disclosure.” Hulu’s only legal argument is its citation to a case about how an online “click-to-accept-terms” form can result in a contract. See id. at 25. The court cannot conclude on this
CONCLUSION

The court GRANTS Hulu’s motion for summary judgment on the comScore disclosures and DENIES the motion for the disclosures to Facebook. This disposes of ECF No. 125-4.

IT IS SO ORDERED.

Dated: April 28, 2014

LAUREL BEELE
United States Magistrate Judge
Plaintiff Khalilah Wright ("Wright" or "Plaintiff") brings this putative class action against Defendant LinkedIn Corporation ("Defendant" or "LinkedIn"). Presently before the Court is LinkedIn’s Motion to Dismiss Plaintiff’s Second Amended Consolidated Complaint ("SAC"). The Court has fully reviewed the parties’ submissions and heard oral arguments of counsel presented at the hearing on November 22, 2013. For the reasons explained below, the Court has determined that LinkedIn’s Motion will be GRANTED IN PART and DENIED IN PART.
I. BACKGROUND

The following facts are taken from Plaintiff’s SAC. LinkedIn owns and operates the website www.LinkedIn.com, which provides an online community for professional networking.

Prospective members may sign up for a membership by providing a valid email address and registration password, which LinkedIn stores on its database. Once registered, a member may create a free online professional profile containing such information as employment and educational history.

When members register, they are required to confirm that they agree to LinkedIn’s User Agreement (“User Agreement”) and Privacy Policy (“Privacy Policy”). The Privacy Policy contains a statement that “[a]ll information that you provide will be protected with industry standard protocols and technology.”

For a monthly fee, members can upgrade to a paid “premium” subscription which grants them increased networking tools and capabilities. Members who purchase a premium subscription agree to the same terms and services of the User Agreement and Privacy Policy as if they were non-paying members.

Plaintiff alleges that sometime in 2012 hackers infiltrated LinkedIn’s computer systems and services. On June 6, 2012, the hackers posted approximately 6.5 million stolen LinkedIn users’ passwords on the Internet. On or around June 9, 2012, LinkedIn released a statement on its blog stating that it had recently completed a switch of its password encryption method from a system that stored member passwords in a hashed format to one that used both salted\(^1\) and hashed\(^2\) passwords for increased security.

Plaintiff alleges that she paid for a premium subscription from March 2010 until approximately August 2010. She alleges that her LinkedIn password was retrieved by the hackers and posted on the Internet on June 6, 2012. She alleges that, prior to her purchase of the premium subscription, her password was stored in a hashed format.

---

1 According to the SAC, “salting” is an encryption process that protects information by concatenating a plaintext password with a series of randomly generated characters prior to hashing.

2 According to the SAC, “hashing” is an encryption process that protects information by applying a one-way function or algorithm to it. Hash functions are designed to reveal no information about the underlying input and are designed such that minor changes in inputs will result in major changes to outputs.
subscription, she read LinkedIn’s User Agreement and Privacy Policy and that, had LinkedIn
disclosed its lax security practices, she would have viewed the premium subscription as less
valuable and would either have attempted to purchase a premium subscription at a lower price or
not at all.

II. LEGAL STANDARDS

a. Motion to dismiss under Rule 12(b)(1)

A Rule 12(b)(1) motion to dismiss tests whether a complaint alleges grounds for federal
subject matter jurisdiction. If the plaintiff lacks standing under Article III of the U.S. Constitution,
then the court lacks subject matter jurisdiction, and the case must be dismissed. See Steel Co. v.

A jurisdictional challenge may be facial or factual. Safe Air for Everyone v. Meyer, 373
F.3d 1035, 1039 (9th Cir. 2004). Where the attack is facial, the court determines whether the
allegations contained in the complaint are sufficient on their face to invoke federal jurisdiction,
accepting all material allegations in the complaint as true and construing them in favor of the party
asserting jurisdiction. See Warth v. Seldin, 422 U.S. 490, 501 (1975). Where the attack is factual,
however, “the court need not presume the truthfulness of the plaintiff’s allegations.” Safe Air for
Everyone, 373 F.3d at 1039. In resolving a factual dispute as to the existence of subject matter
jurisdiction, a court may review extrinsic evidence beyond the complaint without converting a
motion to dismiss into one for summary judgment. See id.; McCarthy v. United States, 850 F.2d
558, 560 (9th Cir. 1988) (holding that a court “may review any evidence, such as affidavits and
testimony, to resolve factual disputes concerning the existence of jurisdiction”). Once a party has
moved to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the opposing party
bears the burden of establishing the Court’s jurisdiction. See Kokkonen v. Guardian Life Ins. Co.,
Cir. 2010).
b. Motion to dismiss under Rule 12(b)(6) and Rule 9(b)

A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A motion to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure tests the legal sufficiency of the claims asserted in the complaint. Fed. R. Civ. P. 12(b)(6); Navarro v. Block, 250 F.3d 729, 731 (9th Cir. 2001). The court must accept all factual allegations pleaded in the complaint as true, and must construe them and draw all reasonable inferences from them in favor of the nonmoving party. Cahill v. Liberty Mutual Ins. Co., 80 F.3d 336, 337–38 (9th Cir. 1996). The Court is not bound, however, to accept “legal conclusions” as true. Ashcroft v. Iqbal, 556 U.S. 662 (2009).

To avoid a Rule 12(b)(6) dismissal, a complaint need not contain detailed factual allegations; rather, it must plead “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). However, “a plaintiff’s obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Id. at 555 (citation omitted). “Factual allegations must be enough to raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true (even if doubtful in fact).” Id. (citation omitted). In spite of the deference the court is bound to pay to the plaintiff’s allegations, it is not proper for the court to assume that “the [plaintiff] can prove facts that [he or she] has not alleged or that defendants have violated the . . . laws in ways that have not been alleged.” Associated Gen. Contractors of Cal., Inc. v. Cal. State Council of Carpenters, 459 U.S. 519, 526 (1983).

But “[w]hen there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief.” Iqbal, 556 U.S. at 679. A claim has “facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. at 677 (citing Twombly, 550 U.S. at 556). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.”
Id. “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it
‘stops short of the line between possibility and plausibility of entitlement to relief.’” Id. (quoting
Twombly, 550 U.S. at 557).

Complaints alleging fraud must satisfy the heightened pleading requirements of Federal
Rule of Civil Procedure 9(b). Rule 9(b) requires that in all averments of fraud or mistake, the
circumstances constituting fraud or mistake shall be stated with particularity. Malice, intent,
knowledge, and other conditions of a person’s mind may be alleged generally. A pleading is
sufficient under Rule 9(b) if it “state[s] the time, place and specific content of the false
representations as well as the identities of the parties to the misrepresentation.” Misc. Serv.
Workers, Drivers & Helpers v. Philco–Ford Corp., 661 F.2d 776, 782 (9th Cir. 1981) (citations
omitted); see also Vess v. Ciba–Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting
Cooper v. Pickett, 137 F.3d 616, 627 (9th Cir. 1997)) (“Averments of fraud must be accompanied
by ‘the who, what, when, where, and how’ of the misconduct charged.”) Additionally, “the
plaintiff must plead facts explaining why the statement was false when it was made.” Smith v.
Allstate Ins. Co., 160 F.Supp.2d 1150, 1152 (S.D. Cal. 2001) (citation omitted); see In re GlenFed,
Inc. Sec. Litig., 42 F.3d 1541, 1549 (9th Cir. 1994) (en banc) (superseded by statute on other
grounds).

Regardless of the title given to a particular claim, allegations grounded in fraud are subject
to Rule 9(b)’s pleading requirements. See Vess, 317 F.3d at 1103–04. Even where fraud is not an
essential element of a consumer protection claim, Rule 9(b) applies where a complaint “rel[ies]
entirely on [a fraudulent course of conduct] as the bases of that claim . . . the claim is said to be
‘grounded in fraud’ or to ‘sound in fraud,’ and the pleading . . . as a whole must satisfy the
particularity requirement of Rule 9(b).” Kearns v. Ford Motor Co., 567 F.3d 1120, 1125 (9th Cir.
III. DISCUSSION

LinkedIn moves to dismiss all claims in the SAC for lack of standing pursuant to Rule 12(b)(1) and failure to state a claim pursuant to Rule 12(b)(6).

The SAC contains three claims for: 1) violation of the fraud prong of California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code, § 17200 et seq., 2) violation of the unfair prong of the UCL, and 3) breach of contract. Plaintiff concedes that her second and third claims should be dismissed and asks that the Court do so without prejudice. Docket No. 87, Pl.’s Opp. Brief at 3. LinkedIn asks that the Court dismiss all three claims with prejudice.

For the reasons explained below, the Court DISMISSES Plaintiff’s second and third claims with prejudice. LinkedIn’s motion is DENIED as to Plaintiff’s first claim.

a. Standing under Article III and the UCL

i. Background

The Court dismissed Plaintiff’s First Amended Complaint (“FAC”) for lack of Article III standing. See Docket No. 72. Plaintiff had attempted to establish standing based on the theories that she had suffered an injury in fact because 1) she did not receive the benefit of her bargain with LinkedIn, and 2) she now faces an increased risk of future harm as a result of the 2012 hacking incident. The Court rejected both standing theories, finding, inter alia, that the promise of industry standard security had not been a part of Plaintiff’s bargain for premium services.

The parties continue to dispute whether Plaintiff has standing under Article III or under the UCL. Plaintiff has abandoned the standing theories she previously advanced and now contends that she has standing because she purchased her premium subscription in reliance on LinkedIn’s misrepresentation and would not have done so but for the misrepresentation. Importantly, the SAC (unlike the FAC) alleges that Plaintiff did, in fact, read and rely upon the statement in the Privacy Policy regarding industry standard security.

With these amendments, the SAC’s allegations are sufficient to confer both standing under Article III and statutory standing under the UCL.
ii. The parties’ positions

The parties essentially divide the UCL standing and Article III standing cases into two categories. Plaintiff relies primarily on a line of cases in which courts find standing under the UCL and under Article III for plaintiffs who purchase deceptively labeled or advertised products in reliance on the misinformation contained in the labels or advertisements.

As to UCL standing, in Kwikset Corp. v. Superior Court, the California Supreme Court held that “[a] consumer who relies on a product label and challenges a misrepresentation contained therein can satisfy the standing requirement of [the UCL] by alleging . . . that he or she would not have bought the product but for the misrepresentation.” 51 Cal. 4th 310, 330 (2011). In Hinojos v. Kohl’s Corp., 718 F.3d 1098 (9th Cir. 2013), the Ninth Circuit Court of Appeals applied Kwikset in “a straightforward manner” to hold that “when a consumer purchases merchandise on the basis of false price information, and when the consumer alleges that he would not have made the purchase but for the misrepresentation, he has standing to sue under the UCL and FAL because he has suffered an economic injury.” 718 F.3d at 1107.

The Article III standing cases in the Ninth Circuit agree that plaintiffs who make allegations similar to those made in Kwikset and Hinojos would also satisfy Article III’s standing requirements. For example, Article III standing has been found for class members who “paid more for [a product] than they otherwise would have paid, or bought it when they otherwise would not have done so, because [the defendant] made deceptive claims and failed to disclose the [product’s] limitations.” Mazza v. Am. Honda Motor Co., Inc., 666 F.3d 581, 595 (9th Cir. 2012) (citing Stearns v. Ticketmaster Corp., 655 F.3d 1013, 1021 (9th Cir. 2011)). Another Ninth Circuit case found Article III standing by applying the rule from Kwikset to the plaintiffs’ allegation that they paid more for a product due to reliance on false advertising. See Degelmann v. Advanced Med. Optics, Inc., 659 F.3d 835, 840 (9th Cir. 2011) vacated, 699 F.3d 1103 (9th Cir. 2012).

LinkedIn, on the other hand, distinguishes the labeling/advertising cases on the basis that the representation in the Privacy Policy was not contained in a label or an advertisement. The Privacy Policy applies to all members, both paying and non-paying and, according to LinkedIn,
was not included or incorporated into the premium services contract that Plaintiff entered into.

Thus, LinkedIn argues, “[u]nder no plausible theory can this single sentence in the Privacy Policy that applies to all LinkedIn members be considered an ‘inducement’ to the purchase of a premium subscription, the ‘advertisement’ of premium services, or an ‘effective marketing technique’ for premium service.” Docket No. 89, Def.’s Reply at 7.

LinkedIn instead points to a number of other consumer cases in which courts have rejected theories of injury in fact that, like Plaintiff’s theory, were premised on payment or overpayment for a product. In LinkedIn’s cases, courts have required plaintiffs to allege “something more” than “overpaying for a ‘defective’ product” in order to establish an Article III injury in fact. In re Toyota Motor Corp., 790 F. Supp. 2d 1152, 1165 n.11 (C.D. Cal 2011); see also Whitson v. Bumbo, 2009 WL 1515597 (N.D. Cal. Apr. 16, 2009); Boysen v. Walgreen Co., 2012 WL 2953069 (N.D. Cal. July 19, 2012); In re McNeil Consumer Healthcare, 877 F. Supp. 2d 254 (E.D. Pa. 2012); Williams v. Purdue Pharma Co., 297 F. Supp. 2d 171 (D.D.C. 2003). Based on these cases, LinkedIn contends that Plaintiff has not alleged sufficient facts to establish Article III standing.

LinkedIn argues that the rationale behind the labeling/advertising cases is that “the overpayment injury does not depend on how the product functions because ‘labels’ and ‘brands’ have independent economic value.” In re Toyota, 790 F. Supp. 2d at 1165 n.11. Based on that rationale, LinkedIn argues, courts in such cases find economic harm when the consumer paid money for a defendant’s product over a competitor’s product due to the mislabeling. Plaintiff makes no such allegations here. She does not allege, for example, that she purchased LinkedIn’s services over another networking website’s services because of the promise regarding industry standard security.

### iii. Application and conclusion

Having carefully considered the cases, the Court finds that Plaintiff has alleged facts sufficient to confer standing. The critical distinction between Plaintiff’s theory of economic injury and the theories of economic injury rejected in LinkedIn’s cited cases is that Plaintiff alleges her
payment or overpayment was caused by LinkedIn’s alleged misrepresentations, which she alleges she read and relied on in making her decision to purchase a premium subscription. The plaintiffs in LinkedIn’s cases did not, or could not, attempt to establish standing under the same theory as Plaintiff’s. In Williams and Whitson, although the plaintiffs alleged that the defendants had made misrepresentations about the products at issue, the plaintiffs failed to allege that they were deceived by or even that they were exposed to the misrepresentations. 297 F. Supp. 2d at 177; 2009 WL 1515597, at *4. Similarly, neither Boysen nor In re McNeil contained allegations that the plaintiffs purchased the product in reliance on the defendant’s misrepresentations. In re Toyota is inapposite because, while the court did require some plaintiffs to allege “something more” than pure economic loss, it did so only for those plaintiffs who were seeking to establish an economic loss based on a “market effect” theory.3 790 F. Supp. 2d at 1165-1166. Plaintiff’s theory is not based on a loss in market value.

The Court recognizes that there are significant differences between the “single sentence” contained in LinkedIn’s Privacy Policy and the labels and advertisements from Kwikset and Hinojos. Notwithstanding these differences, however, the Court finds that the representation in LinkedIn’s Privacy Policy falls within the scope of the labeling/advertising cases.

First, it is not clear that the reach of the Kwikset line of cases is limited only to misrepresentations that are also labels or advertisements. As the California Supreme Court put it, to satisfy the UCL’s standing requirements, “a party must now (1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., economic injury, and (2) show that that economic injury was the result of, i.e., caused by, the unfair business practice or false advertising that is the gravamen of the claim.” Kwikset, 51 Cal. 4th at 322 (emphasis added).

While it is true that the final holding in Kwikset specifically identified the type of “unfair business 3 Some plaintiffs attempted to establish an injury in fact based on a drop in value of their cars. They did not allege experiencing any defects in their cars despite predicating their loss on the drop in value due to the defect. The court agreed that those plaintiffs should allege “something more” and found that they had met this requirement by 1) showing the reduction in trade-in value of their cars in sources such as Kelley Blue Book and 2) alleging that the drop in value followed public awareness of the defect. 790 F. Supp. 2d at 1166.
practice or false advertising” at issue, that holding was an application of the broader rule identified in the preceding sentence of this paragraph. The Kwikset court did not indicate that the requirements for establishing UCL standing would be any different if the challenged misrepresentation was contained in something other than a deceptive product label. And although Kwikset was a California case concerning standing under the UCL, not Article III, the Ninth Circuit cases indicate that plaintiffs whose allegations meet the Kwikset criteria will at least satisfy the Article III injury in fact requirement. See Hinojos, 718 F.3d at 1104, n.3 (“There is no difficulty in this case regarding Article III injury in fact, and neither party suggests otherwise. We have explained that when, as here, ‘Plaintiffs contend that class members paid more for [a product] than they otherwise would have paid, or bought it when they otherwise would not have done so’ they have suffered an Article III injury in fact.”)

Second, even if the Kwikset line of cases was read to apply solely to advertisements and labels, the term “advertisement” is defined broadly under California law. The UCL expressly incorporates the Fair Advertising Law’s (“FAL”) prohibition on unfair advertising as one form of unfair competition. Hinojos, 718 F.3d at 1103 (citing Cal. Bus. & Prof. Code § 17200). The FAL is broadly written and broadly construed, and a wide range of statements can qualify as an advertisement. Cal. Bus. & Prof. Code § 17500; see Chern v. Bank of Am., 15 Cal. 3d 866, 875 (1976). For example, a statement made in a letter denying a borrower’s request for a loan modification qualifies as “advertising.” Gabali v. OneWest Bank, FSB, 2013 WL 1320770 (N.D. Cal. Mar. 29, 2013). Applying one set of standing requirements to labeling/advertising and another set of standing requirements to other types of misrepresentations, as LinkedIn advocates, would be untenable given the lack of distinction California law places between misleading advertising and other forms of misleading statements.

The opinions in Kwikset and Hinojos provided several examples of marketing practices, including meat labeled as kosher and a product advertised as “not available in stores.” Like those

---

4 “A consumer who relies on a product label and challenges a misrepresentation contained therein can satisfy the standing requirement of section 17204 by alleging, as plaintiffs have here, that he or she would not have bought the product but for the misrepresentation.” Id. at 330.
examples, the statement in LinkedIn’s Privacy Policy might be significant only to a small segment
of consumers and many consumers may not even care to read it before making their purchase. Yet
the California Supreme Court and the Ninth Circuit Court of Appeals have indicated that when
those representations are false, a consumer who is induced by them to purchase a product that she
otherwise would not have purchased has standing to bring an action under the UCL in federal
court.

 Applying the cases discussed above, the Court finds that Plaintiff’s allegations are
sufficient to establish standing under the UCL and Article III. She alleges that she purchased her
premium subscription on the basis of LinkedIn’s statement that its users’ data will be secured with
industry standards and technology, she alleges that the statement was false when she read and
relied on it, and she alleges that she would not have made the purchase (or that she would have
negotiated for a lower price) but for the misrepresentation. Her injury (the purchase induced by the
misrepresentation) is fairly traceable to LinkedIn’s conduct because LinkedIn made the
misrepresentation. And finally, her injury is likely to be redressed by a favorable decision because
restitution is an available remedy under the UCL. Cal. Bus. & Prof. Code § 17203.

b. Plaintiff’s first claim: Fraudulent business practices
   i. Stating a claim

To state a claim under either the fraudulent business practices prong of the UCL, it is
necessary only to show that members of the public are likely to be deceived. In re Tobacco II
Cases, 46 Cal. 4th 298, 312 (2009) (internal quotations and citations omitted).

Plaintiff alleges that the representation in the Privacy Policy is likely to deceive the public
because consumers would believe that LinkedIn used a more effective method of securing its users’
data than it actually did.

LinkedIn attacks the materiality of the alleged misrepresentation, arguing that Plaintiff’s
claim should fail as a matter of law because “it is implausible that a single contractual promise in a
Privacy Policy applicable to all members—free, basic-account members and paying, premium-
account members—would be seen as a material inducement leading a reasonable user to upgrade to a premium account.”

A representation is material if a reasonable consumer would attach importance to it or if the maker of the representation knows or has reason to know that its recipient regards or is likely to regard the matter as important in determining his choice of action. Hinojos, 718 F.3d at 1107 (internal quotations and citations omitted). The materiality of a misrepresentation is typically an issue of fact, and therefore should not be decided at the motion to dismiss stage. See In re Steroid Hormone Product Cases, 181 Cal. App. 4th 145 (2010). In some circumstances, courts have found, as a matter of law, that no reasonable consumer could have been misled by the misrepresentation. See Rice v. Fox Broad. Co., 330 F.3d 1170, 1181 (9th Cir. 2003) (false statements on videotape cover were immaterial because videotape cover could not be observed by potential consumer and therefore could not influence the purchasing decision).

LinkedIn points out that Plaintiff fails to allege that, even if LinkedIn had disclosed the fact that it used unsalted, SHA-1 encryption, Plaintiff would have actually understood such a disclosure to mean that LinkedIn was not employing industry standard security. However, Plaintiff does allege that if LinkedIn had disclosed its security protocols, consumers would have learned that those protocols did not meet the “industry standard” through word of mouth or the media. She supports this reasoning by arguing, essentially, that even if the average consumer would not have understood that unsalted, SHA-1 encryption was below the industry standard, the popular media would have found that disclosure newsworthy and would have disseminated the information to consumers.

Given the above, the Court does not find Plaintiff’s claim barred as a matter of law. The only case that LinkedIn has cited on this point is Rice, and in Rice, it was impossible for the representation to deceive a consumer when no consumer could have viewed the representation prior to making a purchase. Here, the representation was available for the public to read, and, as explained below, Plaintiff has alleged a plausible explanation for why it is likely to deceive the public.
ii. Rule 8

LinkedIn contends that the SAC does not satisfy Rule 8 of the Federal Rules of Civil Procedure. A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A court considering a motion to dismiss can choose to begin by identifying pleadings that, because they are no more than conclusions, are not entitled to the assumption of truth. Iqbal, 556 U.S. at 679. While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations. Id. When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief. Id.

1. Whether Plaintiff plausibly alleges that she read LinkedIn’s representation

In the SAC, Plaintiff alleges the following: “Before signing up for her LinkedIn Premium Subscription, Wright—as she always does when signing up for a service online—read and agreed to the [User Agreement] and Privacy Policy and the representations and obligations listed therein.” Plaintiff also alleges that the User Agreement contained an integration clause, and that the User Agreement governing her premium subscription also “incorporated by reference” LinkedIn’s Privacy Policy and advised her to review and comply with the Privacy Policy.

LinkedIn argues that because the User Agreement was not part of the terms of the contract Plaintiff entered into when she signed up for her premium subscription, the terms therefore did not include the “incorporation by reference” term or the advisement to review the Privacy Policy. Because those allegations are false, LinkedIn continues, there is no reason to accept as true the conclusion—that Plaintiff read and relied on the Privacy Policy in purchasing her premium subscription.

However, regardless of whether or not the User Agreement became a part of Plaintiff’s contract for the premium subscription as a matter of contract law, Plaintiff alleges that she read and relied on the User Agreement and the Privacy Policy before purchasing her premium subscription.
Her understanding of contract law has no bearing on her allegation that she read and relied on those documents.

2. Whether Plaintiff plausibly alleges that LinkedIn’s representation was false

LinkedIn argues that Plaintiff’s allegation that LinkedIn failed to use industry standards to encrypt member passwords is conclusory and unsupported. Plaintiff supports this conclusion with the following factual allegations:

1) When Plaintiff purchased her premium subscription, LinkedIn protected its users’ personal information using the SHA-1 hash function. LinkedIn did not salt the information.

2) Since at least 2006, industry standards have required that users’ personal information, and login credentials in particular, be stored in salted and hashed format.

3) The National Institute of Standards and Technology (“NIST”) recommended that all government agencies stop using SHA-1.

4) Salting has been standard encryption practice since the 1970s, and salting and hashing (with a stronger algorithm than SHA-1) together is the preferred industry practice.

5) Three days after the breach, LinkedIn stated that it would transition from a password database system that hashed passwords, i.e. provided one layer of encoding, to a system that both hashed and salted the passwords, i.e. provided an extra layer of protection that is a widely recognized best practice within the industry.

6) The bare minimum practice within LinkedIn’s industry is to “salt” the input before hashing it, preferably with a multi-digit salt long enough to render rainbow tables (a method of encryption-breaking) entirely useless.
7) The more common industry practice is to (1) salt passwords and then hash them using a more recent and secure algorithm than SHA-1, (2) salt the resulting hash value, and (3) then again run the resulting value through a hashing function. Finally, that fully encrypted password should be stored on a separate and secure server apart from all other user information.

LinkedIn points out that “Plaintiff never explicitly alleges that SHA-1 was below industry standards during the class period. She instead alleges that the National Institute of Standards and Technology [NIST] recommended that all government agencies stop using SHA-1.” Docket No. 81, Def.’s Memo ISO MTD at 19 (internal quotations omitted). LinkedIn then cites to an extrinsic document written by the NIST which purportedly states that the use of SHA-1 hashing is acceptable.

However, even assuming that the Court must disregard Plaintiff’s allegations concerning the NIST’s position on the use of SHA-1 hashing, the rest of Plaintiff’s allegations are sufficient to support her conclusion that LinkedIn’s representation was false. She alleges that LinkedIn used a particular security practice, is specific about what that security practice entailed, alleges that LinkedIn’s practice fell below the “bare minimum” security practice in LinkedIn’s industry, and she is specific about what that “bare minimum” security practice entails. Furthermore, LinkedIn does not contend that the phrase “industry standard” amounts to puffery or is otherwise impossible to define.

Accordingly, dismissal for this reason is unwarranted.

3. Whether Plaintiff plausibly alleges that she was denied the benefit of her bargain

Next, LinkedIn contends that Plaintiff “does not plausibly allege that she did not receive all of the benefits that she bargained for,” arguing that the promise of industry standard security was not one of the benefits included in Plaintiff’s bargain because industry standard security is available to all members whether or not they have upgraded to premium memberships. This was
an argument that the Court found convincing and became one of the grounds for dismissal of the FAC.

This contention is less relevant now that Plaintiff no longer seeks to establish standing based on being deprived of the benefit of her bargain. Furthermore, when a plaintiff alleges economic injury based on being induced by misrepresentations to purchase products that she would not otherwise have purchased, the benefit of the bargain defense is permissible only if the misrepresentation that the consumer alleges was not “material.” Hinojos, 718 F.3d at 1107. Thus, LinkedIn’s contention that Plaintiff received all of the benefits she bargained for is not a sufficient basis for dismissal of the SAC.

iii. Rule 9

LinkedIn contends that the SAC’s averments of fraud do not satisfy Rule 9(b) after disregarding the allegations discussed above on Rule 8 grounds. However, these allegations are sufficiently pleaded and must be regarded as true at this stage in the proceedings.

In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Fed. R. Civ. P. 9(b).

Plaintiff’s averments of fraud meet the requirements of Rule 9(b). She alleges that the representation was made in LinkedIn’s Privacy Policy, which she read and relied on prior to purchasing a premium subscription, and she alleges facts that explain why the representation was false. Her allegations are specific enough to give LinkedIn “notice of the particular misconduct which is alleged to constitute the fraud charged so that [it] can defend against the charge and not just deny that [it has] done anything wrong.” Semegen v. Weidner, 780 F.2d 727, 731 (9th Cir. 1985).

c. Plaintiff’s second and third claims

As to the SAC’s second and third claims, the Court limits its decision to whether these claims should be dismissed with or without prejudice.

Dismissal with prejudice and without leave to amend is not appropriate unless it is clear on that the complaint could not be saved by amendment. Chang v. Chen, 80 F.3d 1293, 1296 (9th Cir.
Dismissal with prejudice may be appropriate where a plaintiff presents no new facts but only “new theories” and “provided no satisfactory explanation for his failure to fully develop his contentions originally.” Vincent v. Trend Western Technical Corp., 828 F.2d 563, 570-71 (9th Cir. 1987).

Here, although Plaintiff has added new, critical facts to her complaint (particularly, the allegation that she read LinkedIn’s representation before purchasing her premium subscription), she fails to explain how the new facts affect her second and third claims. She concedes that both claims fall within the scope of the Court’s previous order dismissing the FAC. She provides no explanation for why she should be given another chance to amend those claims, other than that she only became aware that her second and third claims fell within the scope of the previous dismissal order after certain evidence was produced by LinkedIn and that she might discover facts through discovery that would allow her to reassert the claims.

Accordingly, Plaintiff’s second and third claims are DISMISSED with prejudice because allowing for further amendment would be futile.

IV. CONCLUSION

For the foregoing reasons, LinkedIn’s Motion to Dismiss Plaintiff’s Second Amended Consolidated Complaint is GRANTED IN PART and DENIED IN PART. Plaintiff’s second and third claims are DISMISSED with prejudice. LinkedIn’s Motion is DENIED as to Plaintiff’s first claim.

The court schedules this action for a Case Management Conference at 10:00 a.m. on June 6, 2014. The parties shall file a Joint Case Management Statement on or before May 30, 2014.

IT IS SO ORDERED

Dated: March 28, 2014

EDWARD J. DAVILA
United States District Judge
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SBS WORLDWIDE, INC.,

Plaintiff,

v.

DENNIS POTTS and WOODLAND INTERNATIONAL TRANSPORT COMPANY, INC., d/b/a WOODLAND GLOBAL

Defendants.

No. 13 C 6557

MEMORANDUM OPINION AND ORDER

JAMES F. HOLDERMAN, District Judge:

On September 13, 2013, plaintiff SBS Worldwide, Inc. (“SBS”) filed a complaint (“Complaint”) (Dkt. No. 1 (“Compl.”)) against former SBS employee Dennis Potts (“Potts”) and Potts’s new employer, Woodland International Transport Company, Inc., doing business as Woodland Global (“Woodland”) (collectively “Defendants”). SBS seeks injunctive and other relief from Potts and Woodland for alleged violations of the Illinois Trade Secrets Act (“ITSA”), 765 ILCS 1065/2-3, tortious interference with business relationships, unfair competition, and unjust enrichment. (Compl. ¶¶ 62-75, 88-91.) SBS also seeks monetary relief from Potts for breach of fiduciary duty and alleged violations of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, et seq. (Compl. ¶¶ 77-87.) Woodland has moved to dismiss (Dkt. No. 12) the four counts alleged against Woodland (Counts I-III, VI) pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted. Potts has moved to dismiss (Dkt. No. 17) all six counts of SBS’s Complaint for the same reason. In its response to Defendants’ motions to dismiss (Dkt. No. 22 (“Pl.’s Resp.”)), SBS asks this court to impose
sanctions on Potts and Woodland. (Id. at 1-2, 8-10.) For the reasons detailed below, Defendants’ motions to dismiss are granted in part and denied in part, and SBS’s motion for sanctions is denied.

FACTUAL BACKGROUND

At this stage in the litigation, the court must accept the factual allegations in SBS’s Complaint as true and must draw all reasonable inferences in SBS’s favor. Fednav Int’l Ltd. v. Cont’l Ins. Co., 624 F.3d 834, 837 (7th Cir. 2010). The facts set forth below are therefore stated from that perspective.

SBS is a global logistics company specializing in international freight and supply chain solutions. (Compl. ¶ 8.) In the course of business, SBS compiles certain confidential information not publicly available regarding its customers. (Id. ¶ 11.) That information includes the customers’ identities, preferences, services, purchasing history, and “specific information regarding customer relationships.” (Id. ¶ 9.) SBS also compiles confidential sales data, including the prices SBS charges its customers and the profit margins SBS earns on its sales. (Id.) SBS alleges it derives significant economic value from this “confidential customer information” because “the fewer competitors who know its customers and call on them, the better position SBS is in to make sales.” (Id. ¶ 12.) SBS similarly keeps its price and margin information confidential to prevent competitors from underbidding SBS. (Id. ¶ 14.) Ultimately, according to the Complaint, SBS’s confidential customer information is “the type of information that any sales person needs and must use to effectively compete for customers against SBS.” (Id. ¶ 56.)

SBS recognizes its proprietary interest in its confidential information by requiring employees to keep the information confidential, restricting its access to selective employees, and
utilizing security measures such as passwords. (Compl. ¶ 14.) SBS also requires employees to abide by a non-disclosure policy barring employees from misusing trade secrets and other confidential business information. (Id. ¶ 17.) In the spring of 2013, SBS added an additional layer of protection by asking certain sales executives, including Potts, to enter into employment agreements containing restrictive covenants. (Id. ¶ 30.) Potts, however, declined to enter into any employment agreement with SBS. (Id. ¶ 31.)

Potts began his employment at SBS in May of 1998, and prior to his resignation held the position of Business Development Executive. (Compl. ¶¶ 19, 23.) In this role he was responsible for finding new customers and interacting with existing customers to increase sales of SBS’s products and services. (Id. ¶ 25.) Between 2007 and April of 2011, before Potts was demoted to Business Development Executive, he held the position of General Manager of SBS’s Elmhurst office. (Id. ¶¶ 19, 21, 23.) In that role, he was responsible for, among other things, ensuring that employees complied with SBS’s company policies. (Id. ¶ 21.)

Beginning in January of 2011, Potts began forwarding emails containing SBS’s confidential customer information to his personal email account, in violation of SBS’s company policy, and continued to do so until his resignation on July 2, 2013. (Compl. ¶¶ 28, 39.) Before he left, Potts attempted to delete the forwarded emails from his SBS email account. (Id. ¶ 40.) On Saturday, June 15, 2013, Potts entered SBS’s offices and removed a number of SBS files. (Id. ¶ 33.) These files contained documents from management meetings, copies of emails, employee salary information, employee commission reports, and SBS profit reports. (Id. ¶¶ 34-36.) The commission reports contained customer contact details, price quotes, and email exchanges with
customers. (Id. ¶ 36.) The profit reports contained details of shipments, revenues, costs, and profit margins. (Id.) Finally, in anticipation of resigning from SBS, Potts quoted shipping prices to SBS customers that he knew would result in losses to SBS. (Id. ¶ 32.) Potts resigned from SBS on July 2, 2013 and his last day of work was July 3, 2013. (Id. ¶ 41.)

After his resignation, Potts began working for Woodland, which competes with SBS to provide international freight and supply chain solutions. (Compl. ¶ 42.) SBS alleges Potts promised Woodland he would use his knowledge of SBS’s confidential customer information to solicit SBS clients on behalf of Woodland. (Id. ¶ 44.) In July of 2013, Potts fulfilled his promise and solicited business from SBS customer Posterservice, Inc. (“Posterservice”). (Id. ¶ 46.) As part of his proposal to Posterservice, Potts asked Posterservice to provide him with “additional information” so that he could underbid SBS based on his knowledge and possession of SBS’s charge codes. (Id.) SBS claims that because SBS and Woodland use different pricing structures, these charge codes were necessary for Potts to offer Posterservice a better price than SBS. (Id.)

Upon learning that Potts was soliciting business from SBS customers, SBS sent Potts a “cease and desist” letter on July 17, 2013. (Compl. ¶ 48.) The letter directed Potts to stop using the confidential information and documents he took from SBS, return all electronic and other information, and to describe the circumstances of his use and disclosure of SBS’s confidential customer information. (Id. ¶ 49.) SBS also informed Woodland that Potts was using SBS’s confidential customer information to compete “unfairly” on Woodland’s behalf. (Id. ¶ 58.) In response, Potts forwarded to SBS’s counsel “hundreds of emails” he had sent from his SBS email account to his personal email account, and returned to SBS four boxes of documents he
had taken from SBS’s offices. (Id. ¶¶ 50, 53.) SBS alleges the returned emails and documents contained SBS’s confidential customer information, (id. ¶¶ 51, 53), and that Potts has retained certain confidential customer information by failing to return all of the emails he forwarded to his personal account between January of 2011 and July 3, 2013 (id. ¶¶ 52, 54).

Despite returning certain emails and documents, Potts has continued to solicit business from SBS customers using SBS’s confidential customer information. (Id. ¶ 55.) Since his resignation, Potts has convinced multiple SBS customers to do business with Woodland instead of SBS. (Id. ¶ 57.) SBS estimates these former customers accounted for over one million dollars in revenue during 2013. (Id.)

On September 13, 2013, SBS filed this lawsuit against Potts and Woodland. SBS’s Complaint asserts the following four counts against Potts and Woodland: violation of the ITSA (Count I); tortious interference with business relationships (Count II), unfair competition (Count III), and unjust enrichment (Count VI). (Compl. ¶¶ 62, 88-91.) SBS’s Complaint asserts two additional counts against Potts: violation of the CFAA (Count IV) and breach of duty of loyalty (Count V). (Compl. ¶¶ 77-87.) SBS seeks monetary relief and an injunction barring Woodland from employing Potts in any role substantially similar to his General Manager or Business Development Executive roles with SBS, and enjoining Potts from having any further contact with any client or customer of SBS with whom Potts had contact during his employment with SBS. Defendants moved to dismiss all counts alleged in SBS’s Complaint pursuant to Rule 12(b)(6). (Dkt. Nos. 12, 17.) On November 12, 2013, in its response to the motions to dismiss, SBS requested that this court impose sanctions on Potts and Woodland for purportedly
mischaracterizing SBS’s Complaint and misleading this court on the law applicable to SBS’s claims. (Pl.’s Resp. at 1-2, 8-10.)

LEGAL STANDARD

Under the Federal Rules of Civil Procedure, a complaint need contain only “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). The complaint must “give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007) (quoting Conley v. Gibson, 355 U.S. 41, 47 (1957)). Although “detailed factual allegations” are not required, “labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Twombly, 550 U.S. at 555. The complaint must “include sufficient facts ‘to state a claim for relief that is plausible on its face.’” Cole v. Milwaukee Area Tech. Coll. Dist., 634 F.3d 901, 903 (7th Cir. 2011) (quoting Justice v. Town of Cicero, 577 F.3d 768, 771 (7th Cir. 2009)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). In ruling on a Rule 12(b)(6) motion, the court “construe[s] the . . . complaint in the light most favorable to Plaintiff, accepting as true all well-pleaded facts and drawing all possible inferences in his favor.” Cole, 634 F.3d at 903.

ANALYSIS

I. Violation of the Illinois Trade Secrets Act (Count I)

Count I alleges trade secret misappropriation in violation of the ITSA, 765 ILCS 1065/2-3. To state a claim under the ITSA, a plaintiff must sufficiently allege (1) the existence of a trade secret and (2) misappropriation of that trade secret. PepsiCo v. Redmond, 54 F.3d 1262,
1268 (7th Cir. 1995); see also Liebert Corp. v. Mazur, 827 N.E.2d 909, 925 (Ill. App. Ct. 1st Dist. 2005). The ITSA defines a trade secret as information that “(1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.” 765 ILCS 1065/2(d). Examples of information that often fulfills the ITSA’s secrecy requirement include “customer lists that are not readily ascertainable; pricing, distribution, and marketing plans; and sales data and market analysis information.” Mintel Intern. Group, Ltd. v. Neerghen, No. 08 C 3939, 2010 WL 145786, at *11 (N.D. Ill. Jan. 12, 2010) (Dow, J.) (citations omitted).

Defendants contend that SBS fails to plead the elements of its ITSA claim. Defendants argue SBS does not sufficiently allege the existence of a trade secret because its Complaint fails to identify facts showing that SBS’s confidential customer information is actually secret or that SBS took reasonable steps to keep its information confidential. (Dkt. No. 14 (“Woodland Mem.”) at 6-7; Dkt. No. 17 (“Potts Mem.”) at 8-10.) Defendants also argue SBS fails to allege any misappropriation of its alleged trade secrets. (Woodland Mem. at 8-9; Potts Mem. at 10-11.)

A. Existence of a Trade Secret

Although Defendants do not contest that SBS derives economic value from its confidential customer information, they contend Count I fails because the Complaint does not contain plausible facts showing that the identities of SBS’s customers or the prices SBS quotes to its customers are actually secret. (Woodland Mem. at 6; Potts Mem. at 8-9.) In the alternative,
Woodland claims SBS has not alleged facts showing it took reasonable efforts to maintain the secrecy of its customers or the prices they pay. (Woodland Mem. at 7.)

   i. Secrecy

   Defendants contend the allegations contained in SBS’s Complaint undermine any claims of secrecy. Defendants argue that paragraph 12 of the Complaint, which states that “the fewer competitors who know [SBS’s] customers . . . the better,” implies that at least some competitors know the identities of SBS’s customers. (Woodland Mem. at 6; Potts Mem. at 9.) Similarly, Defendants argue the allegations in the Complaint show that SBS, like most businesses, discloses its prices to its customers. (Woodland Mem. at 6-7; Potts Mem. at 9-10; see also Compl. ¶ 46.) Consequently, Defendants argue SBS’s customers and prices cannot form the basis of a claim under the ITSA because they are not secret.

   As an initial matter, SBS’s alleged trade secrets include more than merely the identities of its customers and the prices those customers pay. SBS alleges trade secrets in its “confidential customer information,” which includes “customer lists, customer preferences, services used by its customers, prices charged to customers, profit margins, sales data, specific information regarding customer relationships, and other financial information.” (Compl. ¶ 9.) These categories of information, if not readily ascertainable from a public source but instead developed with a substantial amount of time, effort, and money, may be secrets under the ITSA. See, e.g., Mintel Intern. Grp. Ltd., 2010 WL 145786, at *11 (citing Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d 209, 216 (Ill. App. Ct. 1st Dist. 1995)). Here, SBS alleges its confidential customer information is not known to its competitors or the public and that SBS derives
significant value from the alleged confidentiality. (Compl. ¶¶ 11, 64.) In ruling on a 12(b)(6)
motion, the court must accept as true SBS’s allegation that its confidential customer information
is actually secret. See, e.g., Cole, 634 F.3d at 903.

Defendants’ contention that the Complaint undermines SBS’s claims of secrecy is
unconvincing. The Complaint’s assertion that “the fewer competitors who know [SBS’s]
customers . . . the better” is one of SBS’s reasons for maintaining secrecy (Compl. ¶ 12); it does
not, viewed in the light most favorable to SBS, imply that SBS’s customers are commonly
known by its competitors.

Defendants’ contention that SBS’s pricing structure cannot support an ITSA claim is
similarly unavailing at this stage of the litigation. Defendants are correct that SBS’s prices, on
their own, do not fulfill the secrecy criterion of the ITSA. See Applied Indus. Materials Corp. v.
Brantjes, 891 F. Supp. 432, 438 (N.D. Ill. 1994) (Holderman, J.) (“[P]rice information which is
disclosed by a business to any of its customers, unlike a unique formula used to calculate the
price information which is not disclosed to a business’s customers, does not constitute trade
secret information protected by the [ITSA].”) (citations omitted). But SBS alleges that Potts and
Woodland have paired the price information they solicited from SBS’s customers with Potts’s
knowledge of SBS charge codes. (Compl. ¶ 46.) SBS claims these codes, in conjunction with
Potts’s knowledge of SBS’s pricing structure, have allowed Woodland to underbid SBS. (Id.) In
its response to Defendants’ motions to dismiss, SBS clarified that the codes help Potts “reverse
engineer the confidential pricing formula that SBS” uses for a particular customer. (Pl.’s Resp. at
7.) Whether SBS’s pricing structure is truly a confidential formula or merely a line item
summary of SBS’s overall price is a question of fact which the court cannot resolve on a motion to dismiss. Drawing all inferences in favor of SBS, the Complaint alleges sufficient facts to show that SBS’s confidential customer information, including information regarding its pricing structure, fulfills the secrecy criterion of the ITSA.

**ii. Reasonable Measures to Maintain Secrecy**

Defendants argue SBS’s ITSA claim also fails because the Complaint does not identify actions sufficient to maintain the secrecy of SBS’s confidential customer information. (Woodland Mem. at 7; Potts Mem. at 9-10.) Defendants describe a number of precautions SBS declined to take, such as specially labeling secret information and executing confidentiality agreements with each employee. (Woodland Mem. at 7.) Under the ITSA, however, SBS need not take every imaginable precaution to protect its trade secrets. SBS’s safeguards simply must be reasonable under the circumstances to maintain the secrecy of its information. 765 ILCS 1065/2(d).

SBS alleges it took “reasonable measures to maintain [the] . . . secrecy” of its confidential customer information, (id. ¶ 64), and the Complaint describes those reasonable measures in detail: SBS maintained a non-disclosure policy (id. ¶ 17)\(^1\); SBS kept its confidential customer information behind a password-protected intranet (id. ¶ 15); SBS limited its access to selective

---

\(^1\) Woodland argues SBS’s failure to attach the policy to its Complaint suggests “that the policy is imprecise about what SBS considers secret.” (Woodland Mem. at 7.) The court in ruling on a 12(b)(6) motion may consider any exhibits attached thereto. *Cole*, 634 F.3d at 903 (citing *Thompson v. Ill. Dep’t of Prof’l Reg.*, 300 F.3d 750, 753 (7th Cir. 2002)). A plaintiff’s failure to attach an exhibit does not, as Woodland claims, create a presumption that the well-pled facts in the Complaint are untrue.
employees (id.); and SBS utilized traditional security measures to protect physical documents (id.). These facts, viewed in the light most favorable to SBS, sufficiently allege that SBS took reasonable steps to maintain the secrecy of its confidential customer information. See, e.g., Mintel Intern. Grp., Ltd., 2010 WL 145786, at *11 (finding plaintiff had taken reasonable measures to maintain secrecy by limiting access to a select group of employees and requiring employees to sign non-disclosure agreements); RKI, Inc. v. Grimes, 177 F. Supp. 2d 859, 874-75 (N.D. Ill. 2001) (Denlow, J.) (finding plaintiff had taken reasonable measures to maintain secrecy by providing access on a “need-to-know” basis, keeping it on a password-protected computer database, and requiring employees to sign and acknowledge receipt of a non-disclosure policy).

B. Misappropriation of Trade Secrets

SBS must also allege facts showing that Woodland and Potts misappropriated its trade secrets. Under the ITSA, misappropriation occurs by improper acquisition, unauthorized disclosure, or unauthorized use. 765 ILCS 1065/2(b); Lumenate Techs., LP v. Integrated Data Storage, LLC, No. 13 C 3767, 2013 WL 5974731, at *5 (N.D. Ill. Nov. 11, 2013) (St. Eve, J.) (citing Liebert Corp., 827 N.E.2d at 925). Misappropriation by improper acquisition entails acquisition by improper means, which the ITSA defines as “theft, bribery, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means.” 765 ILCS 1065/2(a). Misappropriation by unauthorized disclosure or unauthorized use requires a defendant to use the alleged trade secrets
or disclose them to others “for purposes other than serving the interests of” the owner of the trade secrets. *Lumenate Techs.*, 2013 WL 5974731, at *4 (citations omitted).

SBS sufficiently alleges that Potts and Woodland misappropriated its trade secrets. In its Complaint, SBS alleges Potts had access to SBS’s trade secrets during his employment as a Business Development Executive (Compl. ¶ 26); Potts forwarded emails containing SBS’s trade secrets to his personal email account (id. ¶ 28); he resigned from SBS on July 2, 2013 and immediately joined a competitor (id. ¶¶ 41-42); on June 15, 2013, less than 17 days before his resignation, Potts surreptitiously entered SBS’s office on a weekend and removed documents containing SBS’s trade secrets in violation of SBS policy (id. ¶¶ 33, 34); before resigning, Potts attempted to cover his tracks by deleting from his SBS email folder the emails he forwarded to his personal account (id. ¶ 40); and Potts used SBS’s trade secrets to poach business from multiple SBS customers (id. ¶¶ 46, 57). Potts claims, contrary to the allegations in the Complaint, SBS did not have a policy prohibiting (1) forwarding emails to personal accounts or (2) removing documents from SBS’s physical offices. (Dkt. No. 24 (“Potts Reply”) at 2.) Potts also contends the emails and files he removed did not contain any trade secrets within the meaning of the ITSA, and that SBS’s failure to attach to its Complaint any documents proving otherwise requires this court to dismiss SBS’s claims. (Potts Mem. at 19.) All of Potts’s arguments raise questions of fact this court cannot resolve on a motion to dismiss. At this stage, the court must accept as true SBS’s allegations that Potts took documents containing trade secrets in violation of SBS policy, attempted to cover his tracks by erasing the evidence, and has
since used the information to poach business from SBS’s former customers. These facts are sufficient to allege misappropriation under the ITSA.

SBS also alleges facts sufficient to show that Woodland misappropriated its trade secrets as well. First, SBS alleges that Woodland hired Potts only after he promised Woodland that he would use his knowledge of SBS’s trade secrets to solicit SBS customers. (Compl. ¶ 44.) This agreement is sufficient to allege a misappropriation because it involves an acquisition of SBS’s trade secrets by improper means. 765 ILCS 1065/2(a) (“[i]mproper means includes . . . inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use”). Second, SBS alleges Woodland used, and continues to use, SBS’s trade secrets despite knowledge that the secrets were acquired by improper means. This too is a misappropriation under the ITSA. See 765 ILCS 1065/2(b)(2)(B)(I) (“[m]isappropriation means . . . (2) disclosure or use of a trade secret of a person without express or implied consent by another person who . . . at the time of disclosure or use, knew or had reason to know that knowledge of the trade secret was . . . (I) derived from or through a person who utilized improper means to acquire it”).

Potts argues that no quid pro quo agreement between Woodland and Potts ever occurred. (Potts Mem. at 5.) This argument, like Potts’s earlier arguments, requires this court to ignore its duty to accept as true all well-pleaded facts in the Complaint. Woodland, on the other hand, challenges the adequacy of SBS’s allegation because it is based “upon information and belief,” which Woodland contends does not satisfy the pleading standards under Fed. R. Civ. P. 11. (Woodland Mem. at 8.) Woodland relies on the Seventh Circuit’s decision in Bankers Trust Co. v. Old Republic Insurance Co., 959 F.2d 677 (7th Cir. 1992), which holds that allegations of
fraud require “reasonable precomplaint inquiry” and are not properly made on “information and belief.” *Id.* at 684. But Woodland ignores the next sentence of *Bankers Trust*, which clarifies that pleading facts on “information and belief” is deficient “unless they were facts inaccessible to the plaintiff.” *Id.* The Seventh Circuit has since held that “allegations . . . cannot be faulted for their reliance on ‘information and belief’ . . . [w]here pleadings concern matters peculiarly within the knowledge of defendants.” *Brown v. Budz*, 398 F.3d 904, 914 (7th Cir. 2005). Although *Brown* predates *Twombly* and *Iqbal*, district courts in this circuit have concluded that nothing in either *Twombly* or *Iqbal* overrules the Seventh Circuit’s holding in *Brown*. See *Shales v. Schroeder Asphalt Servs.*, No. 12 C 6987, 2013 WL 2242303, at *4 (N.D. Ill. May 21, 2013) (Kendall, J.) (finding allegations pled on “information and belief” are not categorically deficient); *Simonian v. Blistex*, No. 10 C 1201, 2010 WL 4539450, at *3 (N.D. Ill. Nov. 13, 2010) (St. Eve, J.) (determining pleading information on “information and belief” is not categorically improper, particularly when information lies uniquely within the control of defendant). Unless Potts used his SBS email account to negotiate the conditions of his employment with Woodland, SBS is unlikely to have access to the evidence supporting its allegation. Thus, as a practical matter, SBS must plead its allegations upon information and belief and is entitled to do so under Fed. R. Civ. P. 11.

SBS further alleges Woodland used and continues to use SBS’s trade secrets to seek out and poach SBS’s customers. (Compl. ¶¶ 45, 46, 55-59.) Specifically, Woodland has availed itself of Potts’s tainted sales efforts despite notice from SBS that Potts’s sales rely on SBS’s stolen trade secrets. Although Woodland argues SBS lacks a good faith belief that Woodland received
or used any SBS information, (Woodland Mem. at 8), SBS’s allegations support such an inference. SBS alleges that Potts stole its trade secrets, immediately began working for Woodland, and within two months poached SBS customers previously unknown to Woodland. These facts are sufficient to allege that (1) Woodland received and benefited from SBS’s trade secrets and (2) knew or had reason to know that Potts had obtained the secrets through improper means. See 765 ILCS 1065/2(b)(1).

Accordingly, for the reasons set forth above, SBS’s Complaint sufficiently alleges (1) the existence of one or more trade secrets and (2) misappropriation of those secrets. The court denies Defendants’ motions to dismiss Count I of SBS’s Complaint.

II. SBS’s Common Law Claims (Counts II, III, V, and VI)

To “supplement its claims under the ITSA,” (Pl.’s Resp. at 5), SBS attempts to allege common law claims against Woodland and Potts, including tortious interference with business relations, unfair competition, and unjust enrichment against both Woodland and Potts (Compl. ¶¶ 69-76, 88-91). SBS asserts an additional claim, breach of duty of loyalty, against Potts. (Compl. ¶ 81-87.) Defendants contend the ITSA preempts all of SBS’s common law claims. (Woodland Mem. at 10; Potts Mem. at 11.) The court agrees in part.

The ITSA “abolishes claims other than those based on contract arising from misappropriated trade secrets, replacing them with claims under the [ITSA] itself.” Hecny Transp. Inc. v. Chu, 430 F.3d 402, 404 (7th Cir. 2005); see also 765 ILCS 1065/8(a) (The ITSA “is intended to displace conflicting tort, restitutionary, unfair competition, and other laws of [Illinois] providing civil remedies for misappropriation of a trade secret.”). In Hecny, however,
the Seventh Circuit narrowly construed the ITSA to foreclose only those claims that rest on conduct alleged to misappropriate trade secrets. *Hecny*, 430 F.3d at 404-05 (“An assertion of trade secret in a customer list does not wipe out claims of theft, fraud, and breach of the duty of loyalty that would be sound even if the customer list were a public record.”); see also *RTC Indus., Inc. v. Haddon*, No. 06 C 5734, 2007 WL 2743583, at *3 (N.D. Ill. Sept. 10, 2007) (Grady, J.) (concluding *Hecny* departs from broad preemptive effect previously accorded to ITSA); *Dominion Nutrition, Inc. v. Cesca*, No. 04 C 4902, 2006 WL 560580, at *4 (N.D. Ill. Mar. 2, 2006) (Hart, J.) (noting *Hecny* “narrowly construed” the preemptive effect of the ITSA). After *Hecny*, the test is whether a plaintiff’s claim would stand if the information at issue were not a trade secret. *Lumenate Techs.*, 2013 WL 5974731, at *7; see also *RTC Indus.*, 2007 WL 2743583, at *3 (holding claims that would lie if information were non-confidential are not preempted by ITSA).

SBS’s claims of tortious interference with business relations, unfair competition, and unjust enrichment cannot survive this test. In an attempt to save its “supplemental” common law claims, SBS argues they “are not based exclusively on misappropriation of trade secrets, but also encompass Defendants’ misappropriation and use of all of SBS’s proprietary and confidential information.” (Pl.’s Resp. at 6.) SBS’s Complaint, however, draws no distinction between information it considers to be trade secrets and information that is merely “proprietary and confidential.” According to the Complaint, SBS considers all of its “confidential customer information” to be “in the nature of trade secrets.” (Compl. ¶ 9.) SBS cannot, for the first time in its response, divide its “confidential customer information” into two separate categories: one to
support its ITSA claim and another to support its “supplemental” common law claims. Alternatively, SBS contends the common law claims “are not based entirely on conduct that constitutes misappropriation of trade secrets under the ITSA.” (Pl.’s Resp. at 5) (emphasis added). But SBS’s Complaint fails to allege any conduct that would give rise to its claims if the information at issue were non-confidential. SBS alleges Defendants contacted its customers (Compl. ¶¶ 45, 46, 55); offered them a better price than SBS (id. ¶¶ 46, 57, 61); and claimed “that Woodland Global’s products and services will be superior to SBS’s [products and services]” (id. ¶ 61). Absent an improper advantage, such as the use of SBS’s trade secrets, this conduct does not constitute tortious interference, unfair competition, or unjust enrichment—it is the hallmark of competition.

The ITSA does not, however, preempt SBS’s claim that Potts breached his duty of loyalty to SBS. Under Illinois law, “an employee owes a duty of fidelity and loyalty to his employer.” *V.I.M. Recyclers, L.P. v. Magner*, No. 03 C 0343, 2005 WL 1745657, at *12 (N.D. Ill. July 21, 2005) (Denlow, J.) (citations omitted). Absent a restrictive contractual provision, however, an employee “has a right to enter into competition with the former employer upon leaving such employ.” *Classic Amenities, Inc. v. Verbeke*, No. 00 C 3326, 2003 WL 21801021, at *2 (N.D. Ill. Aug. 1, 2003) (Grady, J.) (quoting *Lawter Int'l, Inc. v. Carroll*, 451 N.E.2d 1338, 1349 (Ill. App. Ct. 1st Dist. 1983)). Thus, on its own, SBS’s claim that Potts misappropriated its trade secrets is insufficient to survive the preemptive effect of the ITSA. The allegation rests solely on the conduct giving rise to the ITSA claim and would not survive if the information at issue was not confidential, because Potts has no duty to forego post-employment competition with SBS using
publicly-available information. But SBS also alleges that Potts, in anticipation of leaving SBS, intentionally undermined SBS’s business by quoting prices to SBS customers that Potts knew would incur substantial losses. (Compl. ¶ 32.) SBS alleges Potts’s actions served two goals: (1) to ingratiate himself with customers he would be shortly soliciting on behalf of Woodland and (2) to cause financial damage to SBS. (Id.) These actions, along with Potts’s other conduct, are sufficient to state a claim for breach of fiduciary duty. See, e.g., Lumenate Techs., 2013 WL 5974731, at *9 (speaking disparagingly about employer to customers, engaging in a work slowdown, downloading employer’s files onto external drives, and attempting to “cover tracks” constitutes breach of fiduciary duty not preempted by ITSA).

Accordingly, the court grants Defendants’ motions to dismiss SBS’s claims of tortious interference with business relations (Count II), unfair competition (Count III), and unjust enrichment (Count VI) because they are preempted by SBS’s claim under the ITSA. The court denies Potts’s motion to dismiss SBS’s claim for breach of duty of loyalty (Count V) because the claim would stand even if SBS’s various categories of confidential customer information were not trade secrets.

III. SBS’s Computer Fraud and Abuse Act Claim (Count IV)

Count IV alleges Potts intentionally—and without authorization—accessed SBS’s computers, intranet, and email system and emailed SBS’s confidential customer information to his personal email account. (Compl. ¶¶ 28-29, 39, 78.) SBS also alleges Potts attempted to conceal his theft by deleting the outgoing emails from his SBS email account. (Id. ¶ 40.) Notwithstanding Potts’s attempt to cover his tracks, SBS does not allege it lost access to any
information as a result of Potts’s conduct. SBS does, however, allege Potts’s conduct caused a “loss” of at least $5,000, including costs related to damage assessment and mitigation.

To state a claim for a violation of the CFAA, a plaintiff must prove: “(1) damage or loss; (2) caused by; (3) a violation of one of the substantive provisions set forth in § 1030(a); and (4) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)-(V)” Cassetica Software, Inc. v. Computer Scis. Corp., No. 09 C 0003, 2009 WL 1703015, at * 3 (N.D. Ill. June 18, 2009) (Kendell, J.). The “underlying concern of the [CFAA] is damage to data and . . . the statute was not meant to cover the disloyal employee who walks off with confidential information.” Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int’l, 616 F. Supp. 2d 805, 813 (N.D. Ill. 2009) (Hibbler, J.) (quoting Kluber Skahan & Assocs., No. 08 C 1529, 2009 WL 466812, *8 (N.D. Ill. Feb. 25, 2009) (Zagel, J.)) (internal quotations omitted).

Here, SBS does not—and cannot—claim Potts’s conduct caused “damage” within the meaning of the CFAA, because SBS does not allege any data were lost or impaired. The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). Courts in this district have consistently interpreted “damage” under the CFAA to include “the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any diminution in the completeness or usability of the data on a computer system.” See, e.g., Farmers Ins. Exch. v. Auto Club Grp., 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011) (Holderman, J.) (collecting cases). By contrast, downloading and emailing trade secrets is not enough to satisfy the damage requirement of the CFAA. Id.; see also Motorola v. Lemko Corp., 609 F. Supp. 2d 760, 769 (N.D. Ill. 2009) (Kennelly, J.) (“The only
harm [plaintiff] has alleged is the disclosure to a competitor of its trade secrets and other confidential information. The CFAA's definition of damage does not cover such harm . . . .”

Instead, SBS alleges it suffered a “loss” attributable in part to damage assessment and mitigation. (Compl. ¶ 79.) The CFAA defines “loss” as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). District courts in this circuit have construed the term “loss” in different ways. Compare Farmers Ins. Exch., 823 F. Supp. 2d at 854 (“[A] plaintiff can satisfy the CFAA’s definition of loss by alleging costs reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused no damage as defined by the CFAA.”) (citations omitted), with Von Holdt v. A-1 Tool Corp., 714 F. Supp. 2d 863, 875-76 (N.D. Ill. 2010) (Manning, J.) (requiring “damage to the computer or computer system” before a plaintiff can prove “loss” under the CFAA). Courts generally agree, however, that “[c]osts not related to computer impairment or computer damages are not compensable under the CFAA.” Farmer Ins. Exch., 823 F. Supp. 2d at 855 (quoting SKF USA, Inc. v. Bjerkness, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009) (Pallmeyer, J.)) (additional citations omitted); see also Cassetica Software, 2009 WL 1703015, at *4 (“With respect to ‘loss’ under the FCAA, other courts have uniformly found that economic costs unrelated to computer systems do not fall within the statutory definition of the term.”); CustomGuide v. CareerBuilder, LLC, 813 F. Supp. 2d 990, 998 (N.D. Ill. 2011) (Holderman, J.) (finding plaintiff failed to state a
CFAA claim by failing to allege “any facts connecting its purported ‘loss’ to an interruption of service of its computer systems”).

Here, SBS fails to allege any facts connecting its purported loss to an interruption of service, loss of data, or even a suspected loss of service or data. Although SBS attributes certain losses to “damage assessment and mitigation,” (Compl. ¶ 79), it is clear from the Complaint that SBS’s “damage assessment” efforts were aimed at determining the scope of information Potts emailed to himself and disclosed to Woodland. (Compl. ¶¶ 50-52.) SBS does not allege it ever lost access to any of the information contained in Potts’s emails, notwithstanding Potts’s attempt to conceal his conduct by deleting the emails. (Compl. ¶ 40.) To be sure, assessing the extent of information illegally copied by an employee is a prudent business decision. But the cost of such an investigation is not “reasonably incurred in responding to an alleged CFAA offense,” because the disclosure of trade secrets, unlike destruction of data, is not a CFAA offense. Farmers Ins. Exch., 823 F. Supp. 2d at 854. Accordingly, the costs of investigating Potts’s conduct are not “losses” compensable under the CFAA.

Because SBS’s Complaint fails to allege any damage or loss within the definition of the CFAA, SBS’s Complaint fails to state a violation of the CFAA. Potts’s motion to dismiss Count IV is granted.

IV. SBS’s Request for Sanctions

SBS includes in its response to Defendants’ motions to dismiss a request that this court impose sanctions on Woodland and Potts. (Pl.’s Resp. at 8-10.) SBS contends Defendants’ motions mischaracterize the allegations in the Complaint and mislead this court on the law
applicable to SBS’s claims. Fed. R. Civ. P. 11(c)(2) states that a motion for sanctions must be made separately from other motions—not simply included as an additional prayer for relief contained in another motion—and served as provided in Rule 5. Because SBS failed to comply with the requirements of Rule 11(c)(2), its motion for sanctions is denied.

CONCLUSION

For the reasons explained in this memorandum opinion, the court rules as follows: Defendants’ “Motion[s] to Dismiss” (Dkt. Nos. 12, 17) are denied as to Count I of plaintiff SBS’s Complaint, because Count I sufficiently alleges a violation of the ITSA against both Defendants, and granted as to Counts II, III, and VI, which are preempted by the ITSA. Potts’s “Motion to Dismiss” (Dkt. No. 17) is granted as to Count IV of SBS’s Complaint, because SBS fails to state a claim under the CFAA, and denied as to Count V, because SBS’s Complaint sufficiently alleges Potts breached his duty of loyalty to SBS. Defendants’ answer to Count I and Potts’s answer to Count V are due on or before 2/28/14. Counsel for the parties are requested to meet and confer pursuant to Rule 26(f). Counsel are also requested to file jointly a Form 52 on or before 3/7/14. This case is set for a report on a status and entry of a scheduling order on 3/11/14 at 9:00 a.m. The parties are encouraged to discuss settlement.

ENTER:

JAMES F. HOLDERMAN
District Judge, United States District Court

Date: February 7, 2013
UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[REDACTED]@MAC.COM
THAT IS STORED AT PREMISES
CONTROLLED BY APPLE, INC.

Magistrate Case. No. 14-228 (JMF)

MEMORANDUM OPINION AND ORDER

Pending before the Court is an Application for a search and seizure warrant pursuant to
Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a), (b) and (c) to
disclose certain records and contents of electronic communications relating to an Apple e-mail
address. ¹ Despite this Court’s repeated prior warnings about the use of formulaic language and
overbroad requests that—if granted—would violate the Fourth Amendment, this Court is once
again asked by the government to issue a facially overbroad search and seizure warrant. For the
reasons explained below, the government’s application for a search and seizure warrant will be
denied.

I. Background

As part of an investigation of a possible violation of 41 U.S.C. § 8702 (Solicitation and
Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy) involving a defense contractor, the
government has filed an application for a search warrant (the “Application”) targeting a specific

¹ All references to the United States Code are to the electronic versions that appear in Westlaw or Lexis.
Apple e-mail address. See Application at 3. For purposes of this opinion, the details of the investigation—which remain under seal on the Court’s docket—are irrelevant.  

Following a standard format used by the Department of Justice, the Application is divided into three main parts. The first part provides background and explains the basis for probable cause. The second part—labeled Attachment A—is titled “Place to Be Searched” and specifies the location of Apple, Inc.; it also explains that the “warrant applies to information associated with the e-mail account [redacted]@mac.com which date from [December], 2013, until the present.” Application at 14. Finally, the third part—labeled Attachment B—operates in a bifurcated manner: under the heading “Particular Things to be Seized,” the Application distinguishes between “Information to be Disclosed by Apple” and “Information to be seized by the government.” Application at 15-16.

The government seeks the following:

ATTACHMENT B
Particular Things to be Seized
I. Information to be disclosed by Apple
   To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A: All records or other information stored by an individual using each account, including address books, contact and buddy lists, pictures, and files;

---

2 Because the Clerk’s office does not index filings on ECF for a search warrant application until after an order has been issued granting or denying an application, this opinion cannot reference specific ECF filing numbers.

3 This opinion addresses an investigatory tool related to an ongoing investigation, and the underlying documents must remain sealed for the time being. However, this opinion is intended to be—and shall be—made public, as it discusses the investigation in a sufficiently vague manner such as to avoid compromising the ongoing criminal investigation.


5 As a practical matter, when a Magistrate Judge is presented with a search warrant application, the Judge signs both the application presented by the government and a standard search warrant form propagated by the Administrative Office of the United States Courts. The search warrant form has a space where the “items to be seized” are listed. Instead of specifying the items there, the government or the clerk’s office typically writes in “See Attachment B.” Thus, when the warrant is presented to the target—in this case Apple—that target receives both the form and Attachment B.
a. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken;
b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which each account was created, the length of service, the types of service utilized, the Internet Protocol (IP) address used to register each account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and [sic] of payment (including any credit or bank account number);
c. All records or other information stored by an individual using each account, including address books, contact and buddy lists, pictures, and files;  
d. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and  
e. All records or other information pertaining to including [sic], without limitation, subscriber names, user names, screen names, or other identities, mailing addresses, residential addresses, business addresses, email addresses and other contact information, telephone numbers or other subscriber number [sic] or identity, billing records, credit card or bank account and information about the length of service and the types of service the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form.

II. Information to be seized by the government
All information described above in Section I that constitutes contraband, evidence, fruits and instrumentalities of violations of 41 U.S.C. § 8702 (Solicitation and Receipt of Kickbacks) and 18 U.S.C. § 371 (Conspiracy), between [December], 2013, and the present, including the following:
a. Records, emails, and other information referring or relating to a government investigation involving any or all of the following: [Specific names of individuals and corporations are redacted].

Application at 15-16.

II. Drafting Errors and The Scope of the Government’s Request

It is evident from the sealed affidavit that the government is really after e-mails from December to the present. Nothing in Attachment B, however, explicitly requests that Apple give

---

6 This paragraph is a repeat of the request after the colon in the initial paragraph.
7 This paragraph is also listed twice in the original Application.
the government any e-mails. Strictly read, it instead asks for extensive non-content records about
the account as well as “address books, contact and buddy lists, pictures, and files.” Application at
15. However, under the subheading of “Information to be seized by the government,”
Attachment B states that the government will “seize” relevant “[r]ecords, e-mails, and other
information . . .” Id. at 16 (emphasis added). The Court believes that this confusion was caused
by poor drafting. Compare Application at 15-16 (repeating sections beginning “All records or
other information stored . . .” and “All records pertaining to communications between Apple . .
.”) with Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal
Investigations at 261. After all, the affidavit discusses specific e-mail conversations as the reason
for seeking the warrant; it would be illogical for the government to then not seek these e-mails.

While it is evident from closely reading the Application and its attachments what the
government is really after, it is equally evident that the government is using language that has the
potential to confuse the provider—in this case Apple—which must determine what information
must be given to the government. See In the Matter of the Application of the United States of
America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone
(D.D.C. Oct. 31, 2013) (Facciola, M.J.) (“Generic and inaccurate boilerplate language will only
cause this Court to reject future § 2703(d) applications.”). This Court should not be placed in the
position of compelling Apple to divine what the government actually seeks. Until this
Application is clarified, it will be denied.

III. Analysis

A. The Court’s Previous Actions Regarding Overly Broad Search Warrant Applications
This Court is increasingly concerned about the government’s applications for search warrants for electronic data. In essence, its applications ask for the entire universe of information tied to a particular account, even if it has established probable cause only for certain information. To ameliorate this problem and bring the warrants in line with the Fourth Amendment, this Court has issued “Secondary Orders” to accompany search and seizure warrants for electronic records. These “Secondary Orders” explicitly require that contents and records of electronic communications that are not relevant to an investigation must be returned or destroyed and cannot be kept by the government. See, e.g., In the Matter of the Search of Information Associated with [Redacted] That is Stored at Premises Controlled by Yahoo! Inc., 13-MJ-728, [#4] (D.D.C. Sept. 25, 2013) (sealed) (Facciola, M.J.) (“All contents and records that the United States government determines are not within the scope of Attachment B (II)(A), (B), and (C) shall be either returned to Yahoo!, Inc., or, if copies, destroyed.”). Without such an order, this Court is concerned that the government will see no obstacle to simply keeping all of the data that it collects, regardless of its relevance to the specific investigation for which it is sought. See In the Matter of the Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc., 13-MJ-742, 2013 WL 7856600, at *7 (D.D.C. Nov. 26, 2013) (Facciola, M.J.) (hereinafter “Facebook Opinion”).

That, however, has not been the extent of the Court’s concerns. In the Court’s November 2013 Facebook Opinion involving the search of the Facebook account of Navy Yard shooter Aaron Alexis, the Court raised serious concerns about the government’s use of the two-step procedure under Rule 41 of the Federal Rules of Criminal Procedure. See Facebook Opinion, 2013 WL 7856600, at *6. (“Under that Rule, a warrant ‘may authorize the seizure of electronic
storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or other information consistent with the warrant.”) (citing Fed. R. Crim. P. 41(e)(2)(B)). Under this approach, “the initial section of the warrants authorizing the electronic communications service provider to disclose all email communications (including all content of the communications), and all records and other information regarding the account is too broad and too general.” In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, Nos. 13–MJ–8163, 13–MJ–8164, 13–MJ–8165, 13–MJ–8166, 13–MJ–8167, 2013 WL 4647554, at *1 (D.Kan. Aug. 27, 2013) (“In re App.”). Despite the Court raising its concerns and urging the government to adopt a different approach, the government continues to ask for all electronically stored information in e-mail accounts, irrespective of the relevance to the investigation.

To ameliorate these problems with respect to Alexis’s Facebook account, the Court modified the search warrant to ensure that no third-party communications were turned over to the government, see Facebook Opinion, 2013 WL 7856600, at *3, and to require that the government destroy “[a]ll records and content that the government determines are NOT within the scope of the investigation.” Id. at *7.

While those minimization procedures satisfied the Court in that particular case, it warned the government to “adopt stricter search parameters in future applications” or the Court would be “unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid ‘general’ electronic warrants.” Facebook Opinion, 2013 WL 7856600, at *8. The Court recommended several different approaches, including key word searches, using an independent special master to conduct searches, or segregating the people who are performing the search from those who are conducting the investigation. Id. As the present
Application makes clear, the government has not taken the intervening months to address these concerns. Instead, it persists in its entitlement to the entire email account, without suggesting how the items that may be seized because there is probable cause to believe that they are evidence of a crime can be segregated from those that are not.

**B. The Government Seeks an Unconstitutional General Warrant**

This Court is also troubled that the government seeks a broad search and seizure warrant for e-mails and all other content related to this e-mail account. The Supreme Court has recognized two constitutional protections served by the warrant requirement of the Fourth Amendment. “First, the magistrate’s scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity.” *Coolidge v. N.H.*, 403 U.S. 443, 467 (1971). Thus, it is this Court’s duty to reject any applications for search warrants where the standard of probable cause has not been met. Second, as the Supreme Court has also said, “[T]hose searches deemed necessary should be as limited as possible. Here, the specific evil is the ‘general warrant’ abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings.” *Id.* To follow the dictates of the Fourth Amendment and to avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant application.

With respect to searches of electronic information, careful attention must be paid to the dictates of the particularity requirements of the Fourth Amendment, which limits the “authorization to search to the specific areas and things for which there is probable cause to search.” *Md. v. Garrison*, 480 U.S. 79, 84 (1987). As the Supreme Court has recognized, “the
requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988).

Here, the government has adequately described the “items to be seized” — but it has done so in the wrong part of the warrant and in a manner that will cause an unconstitutional seizure. By abusing the two-step procedure under Rule 41, the government is asking Apple to disclose the entirety of three months’ worth of e-mails and other e-mail account information. See Application at 14-15. Yet, on the very next page, it explains that it will only “seize” specific items related to its criminal investigation; it goes so far as to name specific individuals and companies that, if mentioned in an e-mail, would make that e-mail eligible to be seized. Id. at 15. Thus, the government has shown that it can “describe the items to be seized with [] much specificity”; it has simply chosen not to by pretending that it is not actually “seizing” the information when Apple discloses it. See Facebook Opinion [#5] at 9-10 (“By distinguishing between the two categories, the government is admitting that it does not have probable cause for all of the data that Facebook would disclose; otherwise, it would be able to ‘seize’ everything that is given to it.”).

As this Court has previously noted, any material that is turned over to the government is unquestionably “seized” within the meaning of the Fourth Amendment. See Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989) (noting that a “seizure” occurs when an object is intentionally
detained or taken). The two-step procedure of Rule 41 cannot be used in situations like the current matter to bypass this constitutional reality because the data is seized by the government as soon as it is turned over by Apple. Even if, as Professor Orin Kerr has stated, a search does not occur until “the data is exposed to possible human observation,” Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005), the seizure of a potentially massive amount of data without probable cause has still occurred—and the end result is that the government has in its possession information to which it has no right. See In re App., 2013 WL 4647554, at *9 (“The Court notes that while nothing in Section 2703 or Fed.R.Crim.P. 41 may specifically preclude the government from requesting the full content of electronic communications in a specific email account, the Fourth Amendment may do so and does here.”).

What the government proposes is that this Court issue a general warrant that would allow a “general, exploratory rummaging in a person’s belongings”—in this case an individual’s e-mail account. Coolidge, 403 U.S. at 467. This Court declines to do so.

C. The Electronic Communications Service Provider Should Perform the Search

In the Facebook Opinion, this Court urged the government to adopt a procedure that would allow it to obtain the information it legitimately needs for criminal investigations while respecting the Fourth Amendment, such as:

1. Asking the electronic communications service provider to provide specific limited information such as emails or faxes containing certain key words or emails sent to/from certain recipients;
2. Appointing a special master with authority to hire an independent vendor to use computerized search techniques to review the information for relevance and privilege;
3. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant;
4. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases; and
5. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

See Facebook Opinion, 2013 WL 7856600, at *8 (citing In the Matter of Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW and Information Associated with 12-MJ-9191-DJW Target Email Address, Nos. 12-MJ-8119, 12-MJ-8191, 2012 WL 4383917, at *10 (items 1-2); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Kozinski, J. concurring) (items 3-5)). See also In re Search Warrant, 71 A.3d 1158, 1186 (Vt. 2012) (upholding nine ex ante restrictions on a search warrant for electronic data but holding that the issuing officer could not prevent the government from relying on the plain view doctrine).

Despite being warned to “seriously consider how to minimize the amount of information that its search warrant applications seek to be disclosed” or “find this Court unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid ‘general’ electronic warrants,” Facebook Opinion, 2013 WL 7856600, at *8, the government continues to submit overly broad warrants and makes no effort to balance the law enforcement interest against the obvious expectation of privacy e-mail account holders have in their communications. See United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010) (“Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”). In this case, balancing those interests might require that Apple perform the search for relevant e-mails. Indeed, despite any government protestation, a subpoena served on a third party, such as a bank, compels that entity to look within a record set for the particular documents sought. E-mail providers like Apple are technologically sophisticated actors; in fact, one of Apple’s main
competitors, Google, has created an entire business model around searching the contents of e-mail in order to deliver targeted advertising, and it has done so for a decade. See, e.g., Jon Healey, Privacy Advocates Attack Gmail – Again – for Email Scanning, Los Angeles Times, Aug. 15, 2013, available at http://articles.latimes.com/2013/aug/15/news/la-ol-google-gmail-privacy-reasonable-expectation-20130814 (last visited Mar. 7, 2014) (“As Google notes, this practice has been a standard feature of Gmail since its inception in 2004.”). There is no reason to believe that Apple or any other entity served with a warrant is incapable of doing what entities responding to subpoenas have done under common law.

In its “seizure” section, the Application specifies that e-mails would only be “seized” if they relate to specific people and companies. See Application at 16. On a more fundamental level, the government surely knows how it intends to ultimately sort through the information disclosed by Apple. If a wide disclosure followed by a government search violates the Fourth Amendment, then the obvious answer is to have Apple perform the search using the criteria that the government would itself use in the same way that a bank, in the example used above, might find a particular type of document in its customer files.

This Court is aware that other district courts have held that the “Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.” United States v. Taylor, 764 F. Supp. 2d 230, 237 (D.Me. 2011); accord United States v. Bickle, 10–CR–00565, 2011 WL 3798225, at *20 (D.Nev. July 21, 2011); United States v. Bowen, 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010). But, in light of the government’s repeated submission of overly broad warrants that violate the Fourth Amendment, this Court can see no reasonable alternative other than to require the provider of an electronic
communications service to perform the searches. Under the government’s demand that it be
given everything, the government leaves the Court with only two options: deny the warrants—
thus depriving the government of needed information—or issue warrants that are repugnant to
the Fourth Amendment. Neither is viable.

Thus, having an electronic communication service provider perform a search, using a
methodology based on search terms such as date stamps, specific words, names of recipients, or
other methodology suggested by the government and approved by the Court seems to be the only
way to enforce the particularity requirement commanded by the Fourth Amendment.

D. The Government Must Return or Destroy Irrelevant Information

The Court is particularly troubled that the Application does not specify what will occur
with e-mails and other information that is, even by the government’s standards, not relevant.
Will that information be returned, destroyed, or kept indefinitely? The “Secondary Orders” that
have been routinely issued by this Court—and a significant portion of the Facebook Opinion—
have required the government to destroy all contents and records that are not within the scope of
the investigation as outlined in the search warrant. See Facebook Opinion, 2013 WL 7856600, at
*7. While such a clause in a search warrant application is certainly necessary for its issuance by
this Court, the government should not believe that it is sufficient. In this case, its absence is
grounds enough for the Court to deny the Application.

IV. Conclusion and Order

By the Court’s count, it modified approximately twenty search and seizure warrants for
electronic information during September and December 2013. It will no longer do so. Instead,
any warrants that do not comport with the requirements of the Fourth Amendment will—like the
present Application—be denied with an explanation of why they have been denied so that the
government may have an opportunity to correct its defects. To be clear: the government must stop blindly relying on the language provided by the Department of Justice’s Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual. By doing so, it is only submitting unconstitutional warrant applications.

It is hereby ORDERED that the government’s Application is DENIED without prejudice.

SO ORDERED.

Digitally signed by John M. Facciola
DN: c=US,
email=john_m_facciola@dcd.uscourts.gov, o=United States District Court for the District of Columbia, cn=John M. Facciola
Date: 2014.03.07 12:21:39 -05'00'

JOHN M. FACCIOLA
UNITED STATES MAGISTRATE JUDGE
IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CARNegie STRATEGic DESIGN
ENGINEERS, LLC, )

Plaintiff, )

) vs. )

SCOTT M. CLOHERTY, JAMES W. BURGER, III, ROY D. POINTEK, ) Civil Action No. 13-1112
SHAWN W. SHANER, and CHRISTINE A. BELOTTI MOYER, )

Defendants. )

MEMORANDUM OPINION

CYNTHIA REED EDDY, United States Magistrate Judge.

I. INTRODUCTION

Presently before the Court for disposition is defendants’ motion to dismiss [ECF No. 7] plaintiff’s complaint. For the following reasons, defendants’ motion to dismiss is granted.¹

II. BACKGROUND

Plaintiff, Carnegie Strategic Design Engineers, LLC, (“plaintiff”) is a “full-service, professional engineering firm having expertise in several major engineering disciplines” and employed the defendants at its Pittsburgh, Pennsylvania office for a time up to approximately fall of 2012. See Compl. [ECF No. 1] at ¶¶ 1-7, 9. Defendants Burger and Piontek were employed

¹ Under the Federal Magistrate Judges Act [“Act”], a Magistrate Judge’s jurisdiction may arise through the consent of the parties. 28 U.S.C. § 636(c). Under the Act, “[u]pon consent of the parties, a full-time United States magistrate judge . . . may conduct any or all proceedings in a jury or nonjury civil matter and order the entry of judgment in the case, when specially designated to exercise such jurisdiction by the district court.” 28 U.S.C. § 636(c)(1). Such a referral gives the magistrate judge full “authority over dispositive motions, conduct of trial, and entry of final judgment, all without district court review.” Roell v. Withrow, 538 U.S. 580, 585 (2003); In re Search of Scranton Hous. Auth., 487 F.Supp.2d 530, 535 (M.D.Pa. 2007). “[S]o long as consent [to Magistrate Judge jurisdiction] is clear and unambiguous, it is effective.” In re Search of Scranton Hous. Auth., 487 F.Supp.2d at 535; Roell, 538 U.S. at 591 (consent may be inferred from parties’ actions). Both parties have consented to Magistrate Judge jurisdiction. See Pl.’s Consent to Magistrate Judge Jurisdiction [ECF No. 14]; Defs.’ Consent to Magistrate Judge Jurisdiction [ECF No. 13]. Therefore, it is appropriate for this Court to decide dispositive motions and to enter final judgment.
by plaintiff as Senior Process Control Systems Engineers until they voluntarily terminated their employment on or about August 13, 2012. Id. at ¶¶3-4. Defendant Shaner was employed by plaintiff as a Process Control/Electrical Technical Specialist until he voluntarily quit on approximately September 12, 2012. Id. at ¶ 5. Defendant Moyer was employed by plaintiff as an Electrical Engineer until she voluntarily quit on or about August 13, 2012. Id. at ¶ 6. Defendant Moyer is also a licensed Professional Engineer. Id. Each defendant unilaterally left plaintiff’s employment to work for plaintiff’s competitor. Id. at ¶ 13.

Plaintiff owns and maintains a password-protected computer system with a file and email server for use in operating its business, storing confidential company and client information and performing work on client projects. Id. at ¶ 11. Each defendant had access to this system and plaintiff limited their access for purposes related to client work on plaintiff’s behalf. Id. at ¶ 15. Upon leaving plaintiff’s employ, each defendant copied and stole “valuable data from plaintiff’s password protected computer system and took that data for use unrelated to his or her subsequent employment [with] plaintiff’s competitor. Pl.s’ Op. Br. [ECF No. 12] at 3. Plaintiff claims that defendants had “no authority to access plaintiff’s password-protected computer system or the data therein for any other purpose, and any such access for purposes other than serving plaintiff was . . . without authorization. Compl. [ECF No. 1] at ¶ 15. All told, defendants took more than 285 Gigabytes of data from plaintiff’s system, including confidential company and customer data. Id. at ¶¶ 22-26; See Pl.’s Op. Br. [ECF No. 12] at 1. Specifically, the data taken by defendants included “detailed company and client information including client project data, engineering drawings, cost estimating data, customer contact information, vendor contact information and other non-public proprietary, business and trade secret information.” Compl. [ECF No. 1] at ¶ 31. In some instances, defendants took data
unrelated to any client work or other matters in which that particular defendant was involved, and plaintiff claims that defendant could not have any possible legitimate business purpose or use for. *Id.* at ¶ 33. Plaintiff claims that the commercial value of the non-public business information taken is worth approximately $10,000,000. *Id.* at ¶ 27. Plaintiff has suffered losses of out-of-pocket expenses in excess of $5,000 related to computer forensic investigation, analysis, review and mitigation of the data breach and theft and also loss of productivity incurred as plaintiff’s senior-level management and in-house staff investigated the data breach and theft. *Id.* at ¶ 34.

Plaintiff asserts that defendant’s retrieval and copying of its data was in direct violation of its employee policies. During their employment, each defendant was given and required to comply with plaintiff’s employee handbook, which set forth employee policies regarding confidentiality of client and customer matters, Internet usage, laptop security, work created by employees, protecting company information, conflicts of interest and code of ethics, outside employment and resignation. *Id.* at ¶ 14.

Plaintiff filed the instant complaint alleging defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (“CFAA”). Plaintiff therefore argues that counter to defendants’ obligation and agreement to return all property owned by plaintiff, the defendants accessed, copied, removed and stole valuable data from Plaintiff’s password-protected computer system and took that data for use unrelated to their employment with plaintiff and for use in connection with their employment by plaintiff’s competitor. Plaintiff argues that defendants “lost all authority to access [p]laintiff’s password-protected computer system the instant they undertook to do so for their own benefit or the benefit of any third person.” Compl. [ECF No. 1] at ¶ 20.

---

2 Plaintiff’s complaint additionally alleged a claim for conversion and the misappropriation of trade secrets and proprietary business information. Those claims have been voluntarily dismissed without prejudice by plaintiff. See Stip. of Dismissal [ECF No. 16].
Moreover, under 18 U.S.C. § 1030(e)(6), “[t]o the extent [d]efendants might otherwise have had any authority to access the data on [p]laintiff’s password-protected computer system, they exceeded their authority by accessing such data for anything other than legitimate business purposes relating to [p]laintiff’s business operations. *Id.* at ¶ 21.

In response to plaintiff’s claims, defendants filed a motion to dismiss setting forth two discrete arguments: (1) plaintiff has not properly asserted damage or loss under the CFAA; and (2) plaintiff has failed to plead that defendants’ access to its computer system was “unauthorized” under the CFAA. *See Br.* in Supp. of Mot. to Dismiss [ECF No. 8] at 2. The Court will address each argument in turn.

III. JURISDICTION

This Court has original jurisdiction over this matter pursuant to 28 U.S.C. § 1331 as the action raises questions of federal law under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (“CFAA”).

IV. STANDARD OF REVIEW

Generally, a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests the legal sufficiency of a complaint. For a complaint to survive a Rule 12(b)(6) challenge, it must include factual allegations that “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 697 (2009). A court in determining whether a complaint meets this standard must read the complaint in the light most favorable to the plaintiff and all well-pleaded facts must be taken as true. *Id.* at 677. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 556 (U.S. 2007)). That a court must accept all factual allegations in a complaint does not apply to legal
conclusions of the complaint. *Iqbal*, 556 U.S. at 678. Additionally, “[t]hreadbare recitals of the elements of a cause of action supported by mere conclusory statements, do not suffice.” *Id.* (citing *Twombly*, 550 U.S. at 555.) (the court is not “bound to accept as true a legal conclusion couched as a factual allegation”)). Accordingly, “a complaint must do more than allege the plaintiff’s entitlement to relief. A complaint has to ‘show’ such an entitlement with its facts.” *Fowler v. UPMC Shadyside*, 578 F.3d 203, 210-11 (3d Cir. 2009). Doing so “does not impose a probability requirement at the pleading stage, but instead simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary element.” *Phillips v. County of Allegheny*, 515 F.3d 224, 232 (3d Cir. 2008) (quoting *Twombly*, 550 U.S. at 556, n.3).

V. ANALYSIS

The CFAA is generally an anti-hacker statute that prohibits unauthorized access or the exceeding of authorized access of computers connected to interstate commerce and subjects such violators to criminal and/or civil liability. *See Dresser-Rand Co. v. Jones*, --- F.Supp.2d ---, ---, 2013 WL 3810859, at *3 (E.D.Pa. July 23, 2013) (“*Dresser-Rand*”); *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D.Ariz. 2008) (“[t]he general purpose of the CFAA was to create a cause of action against computer hackers (e.g., electronic trespassers)”). The scope of the CFAA has been expanded in recent years and “[e]mployers . . . are increasingly taking advantage of the CFAA’s civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer’s computer system.” *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d

---

3 *See* 18 U.S.C. § 1030(e)(2)(B); *U.S. v. Drew*, 259 F.R.D. 449, 457 (C.D.Cal. 2009) (that a computer has been connected to interstate commerce “will always be met when an individual using a computer contacts or communicates with an Internet website”); *Mahoney v. DeNuzzio*, 2014 WL 347624, at *5 (D.Mass. Jan. 29, 2014) (same). It is not challenged that the computers in question were connected to the Internet and used in interstate commerce, therefore plaintiff’s computers were “protected computers” under the CFAA.
The presently applicable CFAA provision provides:

Whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . .

shall be punished as provided in subsection (c) of this section.

18 U.S.C. §1030(a)(4). Thus, there are four elements for a claim under section 1030(a)(4): “(1) defendant has accessed a ‘protected computer’; (2) has done so without authorization or by exceeding authorization as was granted; (3) has done so ‘knowingly’ and with ‘intent to defraud’; and (4) as a result has ‘further[ed] the intended fraud and obtain[ed] anything of value.’” P.C. Yonkers, Inc., 428 F.3d at 508 (quoting 18 U.S.C. § 1030(a)(4)). See also Curran v. Mark Zinnamosca & Associates, 2014 WL 271634, at *6 (M.D.Pa. Jan. 23, 2014).

a. Damages and Loss under the CFAA

First, defendants argue that plaintiff’s complaint should be dismissed for failure to allege damage or loss under the CFAA.

Section 1030(g) of the CFAA authorizes a private cause of action for any person “who suffers damage or loss by reason of a violation” but “only if the conduct involves [one] of the factors set forth in” subsection 1030(c)(4)(A)(i). 18 U.S.C. § 1030(g) (emphasis added). Because Section 1030(g) is disjunctive, a plaintiff meets its burden by showing either loss or damage. Here, plaintiff alleges loss under Section 1030(c)(4)(A)(i)(I) which provides that the loss be to “one or more persons during any one year period . . . aggregating at least $5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i)(I).

4 Although the CFAA imposes criminal penalties, it provides for civil penalties in limited situations in which a person “suffers damage or loss by reason of a violation of” the CFAA. 18 U.S.C. § 1030(g).
The term “loss” under the CFAA is defined as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). Additionally, “district court decisions in the [Court of Appeals for the] Third Circuit have held that to fall within this definition of ‘loss,’ the ‘alleged “loss” must be related to the impairment or damage to a computer or computer system.’” Brooks v. AM Resorts, LLC, 954 F.Supp.2d 331, 338 (E.D.Pa. 2013) (quoting Sealord Holdings, Inc. v. Radler, 2012 WL 707075, at *4 (E.D.Pa. Mar. 6, 2012) (additional citations omitted)). Therefore, loss under the CFAA is compensable if “the cost of remedial measures taken to investigate or repair the damage to the computer, or loss is the amount of lost revenue resulting from a plaintiff’s inability to utilize the computer while it was inoperable because of a defendant’s misfeasance.” Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio, 2011 WL 6088611, at *5 (E.D.Pa. Dec. 7, 2011) (emphasis added).

Here, defendants argue that plaintiff has not properly asserted damage under the CFAA, because the only damages recoverable are (1) the cost of remedial measures taken to investigate and repair damage to the computer system and (2) lost revenue when the damage computer was inoperable. See Br. in Supp. of Mot. to Dismiss [ECF No. 8] at 2. Specifically, defendants argue that plaintiff does not allege that [d]efendants deleted any data or otherwise caused harm to the computer system, nor does it assert that their conduct rendered the system inoperable . . . . [Plaintiff] merely asserts that it retained a computer forensic expert to identify the data that [d]efendant copied for their own benefit. The costs associated with investigating an alleged trade secret misappropriation are not recoverable under the CFAA.
Plaintiff responds that it has adequately pled the loss requirement of the CFAA. This Court agrees that plaintiff has adequately pled loss for the following reasons.

Under the CFAA and persuasive authority authored by our sister courts, plaintiff need not show that their system was rendered inoperable, or that tangible damage was done to their computer system. Plaintiff may show loss by alleging that it expended an amount to investigate whether such damage occurred. See Brooks, 954 F.Supp.2d at 338 (“fees paid to an expert for investigating and remedying damage to a computer may be a cognizable ‘loss’ under the CFAA”); Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro, 2077 WL 1847435, at *5 (W.D.Pa. June 25, 2007) (same). See also A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009) (“the costs of responding to the offense are recoverable including costs to investigate and take remedial steps”). Here, plaintiff relies on the “loss” factor under Section 1030(g) rather than the “damage” factor to state a claim under the CFAA. It claims it expended an amount in excess of $5,000 to conduct a computer forensic investigation, analysis and review and to mitigate the data breach, and incurred a loss of productivity due to the in-house investigation of the data breach. Taken these statements as true, as the Court must at this phase, plaintiff has met the required loss element because these are reasonable costs plaintiff expended in responding to the data breach caused by defendants and conducting a damage assessment. Therefore, plaintiff’s complaint will not be dismissed for failure to show loss.

b. “Exceeding Authorized Access” under the CFAA

Although plaintiff has adequately plead that it incurred a loss under the CFAA due to defendants’ actions, it must still show that defendants either obtained access to the computer without authorization or exceeded their authorized access when they obtained access to copy the data from plaintiff’s computers. For the following reasons, this Court finds that defendants
neither obtained access to the data without authorization nor exceeded their authorized access in copying the files and plaintiff’s complaint is dismissed for failure to state a claim under the CFAA.

To be subject to civil liability under the CFAA, the violator must access a protected computer without authorization, or exceed his authorized access. See 18 U.S.C. § 1030(a)(4). The term “exceeds authorized access” is defined as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). The term “authorization” is not defined under the CFAA, which thus entrusts the courts to interpret the term’s reach. As one court has indicated, courts must “wrestle with the breadth of its meaning as increasingly, employers have used a statute originally designed to punish hackers against disloyal employees. Determining an employee’s authorization to company computer systems is further complicated by the proliferation of employer computer and internet use policies.” Dresser-Rand, 2013 WL 3810859 at *5.

Also complicating this issue is the circuit-split that has arisen as a result of divergent interpretations from deciphering the breadth of the term “authorization.” As our sister court has detailed:

Under the narrow view, an employee given access to a work computer is authorized to access that computer regardless of his or her intent to misuse information and any policies that regulate the use of information. See WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc); LVRC Holdings, LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009). Under the broad view, if an employee has access to information on a work computer to perform his or her job, the employee may exceed his or her access misusing the information on the computer, either by severing the agency relationship through disloyal activity, or by violating employer policies and/or confidentiality agreements. See U.S. v. John, 597
Generally, defendants argue that this Court should follow the reasoning set forth in the Court of Appeals for the Fourth and Ninth Circuits, and district courts in this circuit and apply the narrow interpretation of the statutory language, while plaintiff argues that the Court of Appeals for the Third Circuit has already adopted the majority view in *United States v. Tolliver*, 451 Fed. App’x 97 (3d Cir. 2011); *cert. denied* 133 S.Ct. 105 (2012) (“*Tolliver*”) and this Court should follow suit by applying the broader interpretation of the statute.

Defendants argue that plaintiff has failed to plead that their access to its computer system was unauthorized under the CFAA because other district courts in the Court of Appeals for the Third Circuit when faced with this same issue have held that employees who are authorized to access the data at issue do not “exceed their authority if they copy that data for their own benefit.” *Id.* at *5.* Therefore, because plaintiff concedes the fact that defendants “were authorized to access the information and data that they copied,” defendants

---

5 Academics have labeled these views into three categories as “agency-based authorization, code-based authorization and contract based authorization.” *Dresser-Rand*, 2013 WL 3810859 at *5 (citations omitted).

have not violated the CFAA. *Id.*

Plaintiff responds that civil liability under the CFAA extends to employees who copy data from an employer’s protected computer. Pl.’s Op. Br. [ECF No. 12] at 7. Plaintiff relies heavily on the non-precedential finding in *Tolliver* for this point. In *Tolliver*, the defendant was convicted of violating, inter alia, the CFAA for running a fraudulent check cashing scheme. Tolliver was an employee of a bank and had access to the bank’s computer systems that were used to manage and track its customer accounts. *Tolliver*, 451 Fed. App’x at 99. Tolliver used her own employee number and password to the bank’s computer system to access customer information and used such information to gain access to customer information and allegedly provided it to a third party to be used to create and cash fraudulent checks. *Id.* The Court of Appeals noted that Tolliver had no business purpose to access the customer’s information as “Tolliver was . . . not assigned to contact any of these individuals for sales purposes . . . [and bank] employees were not permitted to look at a customer’s account and personal information without a business purpose.” *Id.* at 100. Plaintiff argues that “the Third Circuit explicitly found that the CFAA’s ‘exceeds authorized access’ provisions apply in circumstances . . . where employees are given access to a protected computer for business purposes but exceed their authorized access to obtain information for unauthorized purposes.” Pl.’s Op. Br. [ECF No. 12] at 10.

This Court finds that the Court of Appeals for the Third Circuit has not explicitly adopted the broader and majority interpretation, and accordingly finds that the narrow interpretation of the CFAA adopted by the Court of Appeals for the Ninth and Fourth Circuits and by district courts in our circuit is the proper interpretation of the statute and the true interpretation of Congress’ intent in enacting the statute.
The entirety of the Court of Appeal’s analysis on the CFAA in Tolliver is as follows:

As already discussed, there was sufficient evidence from which to infer that Tolliver intentionally accessed the customers’ accounts and that she did not have a business purpose to do so. As such, the government established that Tolliver exceeded her authorized access, and we will affirm her conviction for this offense.

Tolliver, 451 Fed. App’x at 103.

The Court had no occasion and did not address the discrete issue at hand. The narrow holding in Tolliver cannot fairly be characterized as an express adoption of the broad interpretation of the CFAA language. The issue in Tolliver was whether the criminal conviction was supported by sufficient evidence. The Court was not asked to address the breadth of the term “authorization.” Tellingly, the opinion in Tolliver, which was decided in the midst of circuit split described above, did not reference that fact. The Court did not cite to or discuss cases in which the broad view or the narrow view of the language in the CFAA was at issue. Thus, this Court declines to find that the Court of Appeals for the Third Circuit “expressly” adopted the broader interpretation of the CFAA or to extend the holding in Tolliver, especially in light of the non-precedential status of that decision. See In re Grand Jury Investigation, 445 F.3d 266, 276 (3d Cir. 2006); Gilmore v. Ford Motor Co., 2013 WL 869382, at *1 (W.D.Pa. March 7, 2013).

In addition, the narrow interpretation of the CFAA, as applied by the district courts in this circuit, provides persuasive authority that the term “authorization” should be so interpreted.

In Brett Senior & Associates, an employee before resigning from the plaintiff-employer copied certain confidential business information from the employer’s system to an external hard drive and the court held as a matter of law that he did not exceed his authorized access because “[h]e did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter.” Brett Senior & Assoc., P.C. v. Fitzgerald, 2007 WL 2043377, at
In so finding the court stated that the conduct targeted by the CFAA “is the unauthorized procurement or alteration of information, not its misuse or misappropriation. Because there is no allegation that [defendant-employee] lacked authority to view any information in the [employer’s] computer system, the CFAA claim fails.” *3 (internal citations omitted).

Subsequently, in *Consulting Professional*, the court dismissed a claim under the CFAA against a former employee who was permitted to access the plaintiff-employer’s computer system for use in her employment. *Consulting Professional Resources, Inc. v. Concise Technologies LLC*, 2010 WL 1337723, at *5 (W.D.Pa. March 9, 2010). Again, the employee copied her employer’s confidential information from the employer’s computer system to use at her new company before resigning. *Id.* The court dismissed the claim because it found that the employee’s access to her employer’s computer system did not exceed her authorization under the CFAA. *Id.* The court found that because the employer admitted that the employee had access to the confidential information accessed, and argued that the employee violated her employment contract to obtain confidential information only for business purposes, this was not enough to state a claim under CFAA. *Id.* It found that “[w]hile disloyal employee conduct might have a remedy in state law, the reach of the CFAA does not extend to instances where the employee was authorized to access the information he later utilized to the possible detriment of his former employer.” *Id.* at *6.

Finally, in *Dresser-Rand*, the former-employees/defendants accessed their work laptops and downloaded thousands of documents to external storage devices. *Dresser-Rand*, 2013 WL 3810859 at *9. The court found that if the defendants “were authorized to access their work laptops and to download files from them, they cannot be liable under the CFAA even if they
subsequently misused those documents to compete against” the plaintiff. *Id.* As for the employer’s policies limiting its computers and system to be used only for legitimate business purposes, the court found that such policies governed use and not access of the computers. *Id.*

In coming to this conclusion, the *Dresser-Rand* court conducted a thorough analysis of both the majority and minority views and found that the narrow interpretation of “without authorization” and “exceeds authorized access” applied. It stated:

Courts that adopt the narrow view base their reasoning on the plain language of the statute, dictionary definition of “authorization,” and the rule of lenity. The Fourth Circuit goes through this analysis for a factual scenario very similar to this case. A [former] employee emailed downloaded confidential [company] documents to a personal computer prior to resigning from the company to work for one of its competitors. *WEC Carolina [Energy Solutions LLC v. Miller]*, 687 F.3d [199,] 202 [(4th Cir. 2012)]. The employee allegedly used the downloaded information to make a presentation on behalf of the competitor to a potential [company] customer, and won the projects for the competitor. *Id.* [The employer] had given the employee a laptop computer and authorized access to the company’s intranet and servers. *Id.* [The employer] has policies “prohibiting the use of any confidential information and trade secrets unless authorized” and prohibiting the “download[ing] [of] confidential and proprietary information to a personal computer. *Id.* at 206-07. Yet [the employer] alleged in its complaint that defendant “had access to [the employer’s] intranet and computer servers and to numerous confidential and trade secret documents stored on these computer servers.” *Id.* at 207.

The Court began with examining the plan language of the statute. *Id.* at 203. It recites the Oxford English Dictionary definition for “authorization”: “formal warrant, or sanction.” *Id.* at 204. Citing the Ninth’s Circuit’s analysis in *LVRC Holdings, LLC v. Brekka*, the [Fourth Circuit] concluded that “an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer,” and employee is “without authorization” when “he gains admission to a computer without approval,” and an employee “exceeds authorized access” “when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access.” *Id.* at 204
(citing LVRC Holdings LLC, v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)). These definitions do not extend to the improper use of information validly accessed. Id. at 204. Thus, the [Fourth Circuit] concluded that while defendants may have misappropriated information, they did not access a computer without authorization or exceed their authorized access. Id. at 207.

As for an ambiguity surrounding the term “without authorization,” the Court noted that its interpretation would apply to both the civil and criminal parts of the statute, and therefore any ambiguity would be resolved in favor of lenity. Id. at 204. This rule ensures that we are shielded from unexpected criminal consequences of ambiguous statutes. Id. As a result, the Court was “unwilling to contravene Congress’s intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy.” Id. at 207.

Id. at *6 (internal citations and quotations omitted) (emphasis added). Therefore, based on this interpretation, the court found that “[t]he statute simply does not support a broad interpretation of ‘authorization’ based on employer use policies.” Id. at *8.

Here, plaintiff admits that each defendant was permitted to access its computer system and network and was permitted to access the data at issue. Compl. [ECF No. 1] at ¶ 15. Plaintiff does not allege that defendants “hacked into” a computer or the files that they were not otherwise permitted to access. Rather, the crux of plaintiff’s argument is that rejected by the Consulting Professional court – that defendants lost the right to access such information when they did so for their own or a third parties benefit, and to the detriment of plaintiff. Such a finding is

---

7 The Dresser-Rand court also explained the reasoning used by the Court of Appeals for the Ninth Circuit adopting a narrow interpretation of the statute in U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc). The Nosal court posited its analysis on the seemingly innocuous scenarios that would be criminally and civilly punishable should a court broadly interpret “authorization.” Nosal, 676 F.3d at 860. The court opined: “[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family member from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the New York Times to read at work, but they’d better not visit ESPN.com. And Sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.” Id. This Court shares the sentiment of the Court of Appeals for the Ninth Circuit in that broadly applying the CFAA “would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute.” Id. at 857.
contrary to the plain language of the statute that governs “access” and not “use.”

This Court finds that plaintiff has failed to state a claim for a violation of the CFAA because defendants’ conduct, as alleged, does not claim that defendants either accessed their computers without authorization or exceeded their authorized access. Plaintiff cannot state a claim under the CFAA by transforming its employee policies which prohibited the using of the computer system for anything other than business purposes into a violation of the CFAA. Plaintiff does not claim that defendants gained admission to a computer without its approval or that they used their access to obtain information that falls outside the bounds of approved access. That defendants obtained information that could not have been used for any bona fide business purpose does not fall within the scope of exceeding authorized access if the employee is permitted to otherwise access the data.

While defendants may have misappropriated plaintiff’s business information, they did not access a computer without authorization, nor did they exceed their authorized access. Plaintiff’s statement that “[d]efendants lost all authority to access [its] password protected computer system the instant they undertook to do so for their own benefit or the benefit of any third person” and “[t]o the extent defendants might otherwise have has any authority to access the data on [p]laintiff’s password-protected computer system, the exceeded their authority by accessing such data for anything other than legitimate business purposes relating to Plaintiff’s business operations” are legal conclusions couched as factual assertions properly disregarded by this Court. Compl. [ECF No. 1] at ¶¶ 20-21. The scope of the CFAA does not extend to employees who were authorized to otherwise access the data in question, but did so in bad faith or to the future detriment of his former employer because the this Court interprets the term “authorization” narrowly and finds that it does not extend to the improper use of information
validly accessed.

Accordingly, defendants’ motion to dismiss plaintiff’s complaint for failure to state a claim under the CFAA is granted and plaintiff’s claim is dismissed with prejudice.

VI. CONCLUSION

For the foregoing reasons, defendants’ motion to dismiss plaintiff’s complaint is granted and plaintiff’s claim for a violation of the CFAA is dismissed with prejudice. An appropriate Order follows.

Dated: March 6, 2014

/s Cynthia Reed Eddy
Cynthia Reed Eddy
United States Magistrate Judge

cc: all counsel of record
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE GOOGLE ANDROID CONSUMER PRIVACY LITIGATION

ORDER GRANTING, IN PART, AND DENYING, IN PART, MOTION TO DISMISS SECOND AMENDED COMPLAINT AND SETTING CASE MANAGEMENT CONFERENCE

No. 11-MD-02264 JSW

(Docket No. 62)

This matter comes before the Court upon consideration of the motion to dismiss filed by Defendant Google, Inc. (“Google”). The Court has considered the parties’ papers, relevant legal authority, and the record in this case, and it HEREBY GRANTS, IN PART, AND DENIES, IN PART, Google’s motion to dismiss.

BACKGROUND\(^1\)

Plaintiffs, Kendrick Cochran (“Mr. Cochran”), Nicholas Lawrence (“Mr. Lawrence”), Beverly Julia Levine Hillman-Seidner (“Ms. Hillman-Seidner”), Joan Smith (“Ms. Smith”), Phillip Hall (“Mr. Hall”), and Maritsa Urias (“Ms. Urias”) (collectively “Plaintiffs”) allege that Google “gained and allowed third parties to have unauthorized access to, and engaged in unauthorized use of,” their mobile devices, which use Google’s Android Operating System (“AOS”). (Docket No. 54, Second Amended Consolidated Class Action Complaint (“SACC”), ¶ 2; see also id. ¶¶ 35-46.)

\(^1\) A more detailed account of the facts underlying this dispute is set forth in the Court’s Order granting in part and denying in part the motion to dismiss the First Amended Class Action Complaint. In re Google Android Consumer Privacy Litig., 2013 WL 1283236, at *1-*2 (N.D. Cal. Mar. 26, 2013) (“In re Google”).
According to Plaintiffs, they each installed one or more of the following software applications (“Apps”) on their Android mobile devices: Foursquare; Groupon; Advanced Task Killer; Angry Birds; and Pandora. Plaintiffs allege that these Apps “collected personal data from their Android Mobile Phones and shared this data with” Google. (Id. ¶¶ 4, 78-87.) Plaintiffs contend that they were unaware of and did not knowingly consent to collection of this data, which included

Class Members’ home and workplace locations and current whereabouts; several universally unique device identifiers (“UUIDs”) assigned to Plaintiffs’ Android mobile phones; other device-specific data that was useful to Google and third parties for purposes of “device-fingerprinting;” (i.e., the creation of a back-up unique identifier to engage in tracking of a particular device); along with personal information about Plaintiffs such as their gender and age, what functions Plaintiffs performed on Apps, search terms entered, and selections of movies, songs, or restaurants. (Id. ¶¶ 7-8; see also id. ¶¶ 70-77.)

Plaintiffs allege that although Google claimed users could “opt-in” to location tracking, Google actually continually stored their location data, which was transmitted to Google the next time location services were turned on. (Id. ¶ 73.) Plaintiffs also allege that “Google falsely claims that once users opt-in, they will be ‘anonymized’,” because, in truth, “any location data that is sent back to Google location servers is tied and/or traceable to a specific user through the use of UUID’s.” (Id. ¶ 73; see also id. ¶ 30.) Plaintiffs also assert that Google made a number of misrepresentations about the fact that “their personal information would be kept secure,” which led Plaintiffs to believe that Google would not collect and share “their personal information, including their phone use habits and their location.” (Id. ¶¶ 106-115.)

According to Plaintiffs, “this surreptitious use of resources had a real cost to Plaintiffs ... through the consumption and use of battery life, bandwidth, and file storage of their Android Mobile Phones,” and they contend that Google “potentially” exposed them to data overage charges. (Id. ¶¶ 9-14, 98-105.) Plaintiffs also allege that they paid more for their Android Mobile Phones than they would have paid if they had known Google tracked and shared their personal data. (Id. ¶ 13.)
Based on these and other allegations, which the Court shall address as necessary, Plaintiffs bring claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C. section 1030 (the “CFFA Claim”) and violations of California’s Unfair Competition Law, California Business and Professions Code sections 17200, et seq. (the “UCL Claim”).

ANALYSIS

A. Applicable Legal Standards.

1. Federal Rule of Civil Procedure 12(b)(1) (“Rule 12(b)(1)”).

Google moves to dismiss on the basis that Plaintiffs lack standing under Article III of the United States Constitution. The Court evaluates the motion to dismiss for lack of Article III standing pursuant to Rule 12(b)(1). See White v. Lee, 227 F.3d 1214, 1242 (9th Cir. 2000). A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may be “facial or factual.” Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). In this case, Google raises a facial challenge to Plaintiffs’ standing, and, therefore, the Court “must accept as true all material allegations in the complaint, and must construe the complaint in” Plaintiffs’ favor. Chandler v. State Farm Mut. Auto Ins. Co., 598 F.3d 1115, 1121-22 (9th Cir. 2010); see also Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) (“At the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss, [courts] presume that general allegations embrace those specific facts that are necessary to support the claim.”) (internal cite and quotations omitted).

“The jurisdictional question of standing precedes, and does not require, analysis of the merits.” Equity Lifestyle Props., Inc. v. County of San Luis Obispo, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008). Thus, the fact that Plaintiffs may allege facts that, at the pleading stage, satisfy the requirements for Article III standing does not mean these same facts would be sufficient to state a claim. See Doe v. Chao, 540 U.S. 614, 624-25 (2004); In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 n.5 (N.D. Cal. 2011) (quoting Doe, 540 U.S. at 624-25).

2. Federal Rule of Civil Procedure 12(b)(6) (“Rule 12(b)(6)”).

Google also moves to dismiss each of Plaintiffs’ claims pursuant to Rule 12(b)(6). A motion to dismiss is proper under Rule 12(b)(6) where the pleadings fail to state a claim upon
which relief can be granted. In addition, “lack of statutory standing requires dismissal for failure to state a claim[.]” Maya v. Centex Corp., 658 F.3d 1060, 1067 (9th Cir. 2011). On a motion to dismiss under Rule 12(b)(6), the Court construes the allegations in the complaint in the light most favorable to the non-moving party and takes as true all material allegations in the complaint. Sanders v. Kennedy, 794 F.2d 478, 481 (9th Cir. 1986).

Even under the liberal pleading standard of Rule 8(a)(2), “a plaintiff’s obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007) (citing Papasan v. Allain, 478 U.S. 265, 286 (1986)). Rather, a plaintiff must instead allege “enough facts to state a claim to relief that is plausible on its face.” Id. at 570. “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.... When a complaint pleads facts that are merely consistent with a defendant’s liability, it stops short of the line between possibility and plausibility of entitlement to relief.” Ashcroft v. Iqbal, 556 U.S.662, 678 (2009) (quoting Twombly, 550 U.S. at 557) (internal quotation marks omitted).

If a plaintiff’s allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. See, e.g., Reddy v. Litton Indus., Inc., 912 F.2d 291, 296 (9th Cir. 1990); Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc., 911 F.2d 242, 246-47 (9th Cir. 1990).

B. The Court Denies Plaintiffs’ Motion to Strike.

In support of its motion, Google submitted a declaration from Michael H. Rubin, to which it has attached the following exhibits: (1) the Google Privacy Policy dated October 20, 2011; (2) the Android Market Developer Distribution Agreement; (3) and privacy policies and permissions tabs for the Angry Birds, Foursquare, Groupon, Pandora, and Advanced Task Killer Apps. (Docket No. 63.) Plaintiffs move to strike the declaration and the exhibits in their entirety.

Under the “incorporation by reference” doctrine, courts may consider documents that are “referenced extensively in the complaint and [are] accepted by all parties as authentic,” even
if they are not attached to the complaint. *Van Buskirk v. Cable News Network, Inc.*, 284 F.3d 977, 980 (9th Cir. 2002). The Court denies the motion to strike Exhibit A, which is Google’s Privacy Policy. Plaintiffs quote from that document in the SACC, rely on it to support their claims, and have not disputed its authenticity.

Because the Court did not rely on any of the other exhibits to resolve the motion, the Court denies, as moot, the motion to strike these exhibits.

C. The Court Denies the Motion to Dismiss for Lack of Article III Standing.

In order to satisfy Article III’s standing requirements, Plaintiffs must show: (1) they suffered an “injury in fact” that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that the injury is fairly traceable to Google’s conduct; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560-61.

Plaintiffs argue that they have Article III standing based on, *inter alia*, the increased rate at which their batteries discharge, which impaired the performance of their phones. The Court previously concluded that these allegations were sufficient to establish Article III standing against Google. *See In re Google*, 2013 WL 1283236, at *5. Google argues that the Court should revisit this ruling. Google may not have manufactured Plaintiffs’ mobile devices, and Plaintiffs may face an uphill battle proving this theory of standing.\(^2\) they have alleged sufficient facts to show that they suffered an injury, the injury is fairly traceable to Google’s conduct, and the injury could be redressed by the relief Plaintiffs seek.

Accordingly, the Court denies, in part, Google’s motion to dismiss.\(^3\)

D. The Court Grants Google’s Motion to Dismiss the CFAA Claim.

In their first claim for relief, Plaintiffs assert that Google violated the CFAA. “The CFAA prohibits a number of different computer crimes, the majority of which involve


\(^3\) Because the Court concludes that these facts are sufficient to allege Article III standing, it does not address Plaintiffs alternative theories of standing in this section. The Court shall address those alternative theories, as necessary, in its analysis of the CFAA and UCL claims.
accessing computers without authorization or in excess of authorization, and then taking
specified forbidden actions, ranging from obtaining information to damaging a computer or
computer data.” LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1131 (9th Cir. 2009); see also

In order to bring a civil action under the CFAA, Plaintiffs must be able to show a
damage or loss “to 1 or more persons during any 1-year period ... aggregating at least $5,000 in
value.” 18 U.S.C. § 1030 (c)(4)(A)(i)(I), (g). The CFAA defines “damage” as “any impairment
to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. §
1030(e)(8). The CFAA defines “loss” as “any reasonable cost to any victim, including the cost
of responding to an offense, conducting a damage assessment, and restoring the data, program,
system, or information to its condition prior to the offense, and any revenue lost, cost incurred,
or other consequential damages incurred because of interruption of service.” 18 U.S.C. §
1030(e)(11).

Google argues that Plaintiffs’ allegations are insufficient to show the requisite damage
or loss. Plaintiffs rely on the same factual allegations that purport to show Article III standing
to support the “damage” and “loss” elements of the CFAA Claim. (See SACC ¶¶ 137, 147,
149.) For example, Plaintiffs rely on allegations that Google’s conduct diminished the value of
their PII and, as a result, they suffered loss. (SACC ¶ 149.) For the reasons set forth in its
Order granting in part and denying in part Google’s motion to dismiss the First Amended Class
Action Complaint, the Court concludes that these allegations still are insufficient to establish
damage or loss under the CFAA. See In re Google, 2013 WL 1283236, at *4, *7-*8.

Plaintiffs also rely on the allegations regarding diminished battery life, and they claim
they have sufficiently alleged damage and loss, because their service was interrupted as a result
of Google’s conduct. Plaintiffs contend these allegations distinguish this case from In re
case, the court found that plaintiffs had not included facts to suggest the defendant’s conduct
“impaired” their devices or interrupted service and, thus, failed to show damage or loss under
the CFAA. See id., 844 F. Supp. 2d at 1067. Here, Plaintiffs do allege that Google’s conduct
That fact distinguishes this case from the facts in the related case Yunker v. Pandora Media, 13-CV-3113-JSW. That fact might be sufficient to satisfy the definition of “damage” set forth in 18 U.S.C. section 1030(e)(8). However, in order to pursue a civil action under the CFAA, Plaintiffs also must show economic damage or loss in the amount $5,000. 18 U.S.C. § 1030 (c)(4)(A)(i)(I). Plaintiffs allege that a new battery could cost $70.00. However, none of the Plaintiffs allege that they did purchase new batteries because of Google’s conduct. (See, e.g., SACC ¶¶ 98-102.) The Court concludes that the allegations regarding diminished battery life still are insufficient to allege that the economic damage or loss - even if aggregated - would reach the $5,000 threshold required by the CFAA.

Finally, Plaintiffs rely on allegations that they paid for their data plans, and that Google “used or allowed the use of a finite amount of” their data plans. Again, none of the named Plaintiffs alleged that they incurred any overage charges. Rather, they only allege that they were “potentially” exposed to overage charges.4 (SACC ¶¶ 103-105.) The Court concludes that the allegations regarding “loss” based on “Data Plan Utilization” are insufficient to allege that the economic damage or loss - even if aggregated - would reach the $5,000 threshold required by the CFAA. See, e.g., iPhone App. Litig. II, 844 F. Supp. 2d at 1067.

Accordingly, the Court grants Google’s motion to dismiss the CFAA Claim. This is Plaintiffs’ third iteration of the complaint, and the Court concludes that any further attempts to amend this claim would be futile.

E. The Court Grants, in Part, and Denies, in Part, Google’s Motion to Dismiss the UCL Claim.

Plaintiff’s second claim for relief is a claim under the UCL, which prohibits “three varieties of unfair competition: practices which are unlawful, unfair or fraudulent.” Daugherty v. American Honda Motor Co., 144 Cal. App. 4th 824, 837 (2006); see also Albillo v. Intermodal Container Services, Inc., 114 Cal. App. 4th 190, 206 (2003) (to state a UCL claim, a “plaintiff must establish that the practice is either unlawful (i.e., is forbidden by law), unfair
(i.e., harm to victim outweighs any benefit) or fraudulent (i.e., is likely to deceive members of
the public)


The UCL also “requires that a plaintiff have ‘lost money or property’ to have standing to
sue. The plain import of this is that a plaintiff now must demonstrate some form of economic
injury.” *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011); see also Cal. Bus. &
Prof. Code § 17204. “California courts have distinguished the UCL standing requirement as
more stringent than the federal Article III standing requirement,” because of the requirement
that a UCL plaintiff have lost money or property. *Pirozzi v. Apple, Inc.*, – F. Supp. 2d –, 2013
WL 4029067, at *5 (N.D. Cal. Aug. 5, 2013). However, there are many ways a plaintiff may
establish economic injury to show standing under the UCL, including “surrender[ing] in a
transaction more, or acquir[ing] in a transaction less, than he or she otherwise would have.”
*Kwikset*, 51 Cal. 4th at 323; see also id. at 325 (allegations of “personal, individualized loss of
money or property in any nontrivial amount” is sufficient to allege injury in fact under UCL).

Google moves to dismiss this claim for lack of statutory standing, and it also argues that
Plaintiffs fail to allege facts that show Google violated the UCL.

1. **Plaintiffs Have Statutory Standing to Pursue the UCL Claim.**

Plaintiffs contend they have standing under the UCL based on the allegations that they
“paid more than they otherwise would have for their phones, lost available data on their data
plans, and suffered diminished battery life.” (SACC ¶ 156.) For the reasons set forth in its
previous Order, the Court concludes that Plaintiffs have alleged sufficient facts to show
standing based on the diminished battery life. *See In re Google*, 2013 WL 1283236, at *8; see

Accordingly, the Court denies, in part, Google’s motion to dismiss.

2. **Plaintiffs Fail to State a Claim Under the Unlawful Prong.**

To state a claim based on the unlawful prong, Plaintiffs must allege that the Google
Defendants’ practices are “forbidden by law, be it civil, criminal, federal, state, or municipal,
statutory, regulatory, or court made.” *Saunders v. Superior Court*, 27 Cal. App. 4th 832, 838-39
(1994). “[A] violation of another law is a predicate for stating a cause of action” under the

Plaintiffs fail to allege facts showing a violation of the CFAA, and they do not identify any other statutes that could support a claim under the unlawful prong. Plaintiffs also have not provided the Court with any authority that the alleged violations of the settlement described in paragraph 20 of the SACC could support this claim.

Accordingly, Plaintiffs fail to state a claim under the unlawful prong, and the Court grants, in part, Google’s motion to dismiss.

3. Plaintiffs State a Claim Under the Unfair Prong.

Google also argues that Plaintiffs fail to state a claim under the unfair prong. Unfair simply means any practice whose harm to the victim outweighs any benefits. Olsen v. Breeze, Inc., 48 Cal. App. 4th 608, 618 (1996). “The court must weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” Gafcon, Inc. v. Ponsor & Assocs., 98 Cal. App. 4th 1388, 1425 n.15 (2002). In iPhone App. Litig. II, the court found that allegations regarding collection and dissemination of personal information, which are similar to Plaintiffs’ allegations, were sufficient to state a claim under the unfair prong. iPhone App. Litig. II, 844 F. Supp. 2d at 1073.

In its previous order, the Court found that Plaintiffs had alleged UCL standing for their claims against Google. It also stated that Plaintiffs could state a claim under this prong, if they were able to allege standing. Because Google is the only remaining defendant, Plaintiffs state a claim under the unfair prong.

Accordingly, the Court denies, in part, Google’s motion to dismiss.


Plaintiffs also assert that the Google’s conduct violates the fraudulent prong of the UCL. (See SACC ¶¶ 162-167.) To state a cause of action under the fraudulent prong of Section 17200, it is necessary only to show members of the public are likely to be deceived; allegations that the fraudulent deception was “actually false, known to be false by the perpetrator and
reasonably relied upon by a victim who incurs damages” are not necessary. *In re Tobacco II Cases*, 46 Cal. 4th 298, 312 (2009).

Google argues that, although Plaintiffs have alleged the purportedly false statements with specificity, they still fail to allege facts showing why the statements were false. It also argues that Plaintiffs’ allegations are directly contradicted by the terms of its Privacy Policy.

The Court finds that Plaintiffs’ allegations are similar to the allegations in *iPhone App. Litig. II*. Specifically, Plaintiffs contend that Google’s representations that users can opt-in to location monitoring is false, because Google continues to track and store information even when the location services feature is turned off. *Cf. iPhone App. Litig. II*, 844 F. Supp. 2d at 1074.

In addition, the plaintiffs allege that contrary to the representations in Google’s privacy policy, Google designed the AOS “to enable and promote the taking of Plaintiffs ... personal information so as to further monetize, for [Google’s] benefit, the advertising potential of AOS-based devices and to advance Google’s revenue model in the wireless/mobile marketplace.” (SACC ¶ 3; *see also id.* ¶ 4 (alleging that Google collected and transmitted PII “for purposes wholly unrelated to the use and functionality of” an Android mobile device or App). These allegations are similar to the allegations made by the “iDevice Class” in *iPhone App. Litig. II*. *See* 844 F. Supp. 2d at 1074.

The Court concludes that these allegations, in combination with the allegations that Plaintiffs relied on these statements and paid more for their mobile devices than they otherwise would have are sufficient to *allege* a claim under the fraudulent prong.

Accordingly, the Court denies, in part, Google’s motion to dismiss.

4. **The Court denies Google’s motion to dismiss the claim for restitution.**

Google also moves to dismiss Plaintiffs’ claim for restitution under the UCL on the basis that, because Plaintiffs did not pay any money to Google, they are asking for “non-restitutionary disgorgement,” which is not an available remedy under the UCL. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1145 (2003). In *Ferrington v. McAfee*, the district court rejected a similar argument, and stated that the “distinction California courts have drawn between restitutational disgorgement and non-restitutionary disgorgement does not turn
on whether Plaintiffs paid money directly to the defendant. It turns, rather, on whether the
profits sought to be disgorged would merely ‘restore the status quo by returning to the plaintiff
funds in which she has an ownership interest’ or would achieve something broader.”  Id., 2010
F.3d 977, 996 (9th Cir. 2006)).

Although Plaintiffs do not allege facts that show they paid money directly to Google, the
Court cannot conclude that Plaintiffs might not be able to show an ownership interest in at least
some of Google’s profits.  Cf. Colgan v. Leatherman Tool Group, Inc., 135 Cal. App. 4th 663,
699 (2006) (a plaintiff can seek money or property as restitution where such “money or property
identified as belonging in good conscience to the plaintiff could clearly be traced to particular
funds or property in the defendant’s possession”) (citation omitted).

Accordingly, the Court denies, in part, Google’s motion to dismiss. However, the Court
shall not preclude Google from renewing this argument as this case progresses.

5. The Court denies the motion to dismiss the non-California plaintiffs.

Google also moves to dismiss the UCL claims brought by Mr. Lawrence, Ms. Hillman-
Seidner, Ms. Smith, Mr. Hall, and Ms. Urias, on the basis that they are not California residents.
In support of this argument, Google relies on Mazza v. American Honda Motor Co., 666 F.3d
In Mazza, the defendant was headquartered in California, and the plaintiffs alleged that the
allegedly fraudulent misrepresentations emanated from California. However, the transactions
that purportedly injured class members took place outside California. Mazza, 660 F.3d at 590.
The Ninth Circuit reversed the district court’s decision to certify a nationwide class for alleged
violations of the UCL, and it held that “[u]nder the facts and circumstances of this case, we hold
that each class member’s consumer protection claim should be governed by the consumer
protection laws of the jurisdiction in which the transaction took place.”  Id. at 594.

Plaintiffs argue that the Mazza argument is premature and should be addressed at the
class certification phase. In the Frezza case, the district court rejected a similar argument, and
found that the choice-of-law principle announced in Mazza “applies generally and is instructive
even when addressing a motion to dismiss.” Frezza, 2013 WL 1736788, at *6; see also id., at *5 (“The factual analogy makes Mazza’s application of the choice-of-law rule to the facts of this case, not only relevant but controlling.”). However, in both Mazza and Frezza, the courts engaged in a choice-of-law analysis to determine which state’s law should apply.

Google raised this argument in a footnote, and it presents no argument as to why Texas and Alabama law would conflict with California law. Accordingly, the Court concludes that Google has not met its burden to show the claims of non-California plaintiffs should be dismissed. This ruling is without prejudice to Google renewing this argument in a subsequent motion.

CONCLUSION

For the foregoing reasons, the Court grants, in part, and denies, in part, Google’s motion to dismiss. The Court ORDERS the parties to appear for a case management conference on April 18, 2014 at 11:00 a.m., in Courtroom 5, Second Floor, 1301 Clay Street, Oakland, California. The parties’ joint case management statement shall be due by no later than April 11, 2014.

IT IS SO ORDERED.

Dated: March 10, 2014

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

In re: SONY GAMING NETWORKS AND CUSTOMER DATA SECURITY BREACH LITIGATION

MDL No.11md2258 AJB (MDD)
As to all member and related cases
ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS’ MOTION TO DISMISS PLAINTIFFS’ FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT
(Doc. No. 135)

This action arises out of a criminal intrusion into a computer network system used to provide online gaming and Internet connectivity via an individual’s gaming console or personal computer. Plaintiffs, a nationwide putative consumer class, allege that Sony Computer Entertainment America, LLC (“SCEA”), Sony Online Entertainment, LLC (“SOE”), and Sony Network Entertainment America, Inc. (“SNE”) (collectively, “Sony” or “Defendants”), failed to provide reasonable network security, including utilizing industry-standard encryption, to safeguard Plaintiffs’ personal and financial information stored on Sony’s network.¹

Presently before the Court is Sony’s motion to dismiss Plaintiffs’ First Amended Consolidated Class Action Complaint (“FACC”). (Doc. No. 135.) Sony also submitted a request for judicial notice, (Doc. No. 135, Ex. 2), a notice of lodgment of foreign authorities, (Doc. No. 135, Ex. 2), and a notice of supplemental authorities, (Doc. No. 137).2 Plaintiffs filed an opposition to Sony’s motion to dismiss on May 6, 2013, (Doc. No. 146), and Sony filed a reply on June 20, 2013, (Doc. No. 150). The Court issued a tentative ruling on October 10, 2013, (Doc. No. 157), and held a hearing on the motion on October 18, 2013, (Doc. No. 158). On October 24, 2013, the Court ordered supplemental briefing on seven of Plaintiffs’ consumer protection claims. (Doc. No. 159.) Sony filed its supplemental brief on November 15, 2013, (Doc. No. 163), Plaintiffs filed their opposition on December 6, 2013, (Doc. No. 164), and Sony filed its reply on December 20, 2013, (Doc. No. 165). On January 7, 2014, Plaintiffs filed a notice of supplemental authority informing the Court of a recent memorandum decision issued by the Ninth Circuit.3 (Doc. No. 166.) For the reasons set forth below, the Court GRANTS IN PART and DENIES IN PART Sony’s motion to dismiss.

BACKGROUND

I. Factual Background

Sony develops and markets the PlayStation Portable hand-held device (“PSP”) and the PlayStation 3 console (“PS3”) (collectively, “Console” or “Consoles”). (FACC ¶¶ 38, 39.) Both Consoles allow users to play games, connect to the Internet, and access

2 Plaintiffs filed a response to Sony’s notice of supplemental authorities on March 20, 2013. (Doc. No. 138.) The document was struck from the record as an improper sur-reply. (Id.) Plaintiffs were instructed to include any opposition to Sony’s notice of supplemental authorities in their opposition. (Id.) Plaintiffs did not subsequently file an opposition to these documents. Accordingly, the Court GRANTS Sony’s motion for judicial notice and considers Sony’s supplemental and foreign authorities in support of the instant motion.

3 The Court does not specifically address Plaintiffs’ submission of the Ninth Circuit’s memorandum opinion in In Re Sony PS3 “Other OS” Litigation. (Doc. No. 166, Ex. A.) The Court did not rely on any language included in the district court’s decision that was subsequently overruled, nor did the Court dismiss Plaintiffs’ UCL, FAL, and/or CLRA claims (the only rulings pertinent here that were reversed by the Ninth Circuit).
Qriocity, Sony Online Entertainment Services, and the Play Station Network (“PSN”) (collectively, “Sony Online Services”).4 (Id. at ¶¶ 40-43.) Through the PSN, which is offered to consumers free of charge, users can engage in multi-player online games, (Id. at ¶ 27), and for additional one-time fees, the PSN allows users to purchase video games, add-on content (“map packs”), demos, themes, movie trailers, TV shows, and movies (collectively, “Downloads”). Users can also access various prepaid third party services by connecting to Sony Online Services via their Consoles or computers, including Netflix, MLB.TV, and NHL Gamecenter LIVE (collectively, “Third Party Services”). (Id. at ¶ 45).

Before establishing a PSN, Qriocity, and/or SOE account, Plaintiffs and other consumers were required to enter into a Terms of Service User Agreement with Sony and agree to Sony’s Privacy Policy. (Id. at ¶¶ 55-60.) As part of this registration process, Plaintiffs and other consumers were required to provide Sony with personal identifying information, including their names, mailing addresses, email addresses, birth dates, credit and debit card information (card numbers, expiration dates, and security codes), and login credentials (collectively, “Personal Information”).5 (Id. at ¶ 35.) On April 1, 2011, SCEA transferred its online PSN and Qriocity service operations to SNEA, including transferring Plaintiffs’ and other Class members’ Personal Information to SNEA for handling. (Id. at ¶ 54.) As a result of the transfer, SNEA required all PSN and Qriocity users to enter into a new Terms of Service User Agreement (“PSN User Agreement”) and Privacy Policy (“PSN Privacy Policy”). (Id. at ¶¶ 55, 56.) Plaintiffs

4 The SOE network is an online gaming network distinct from the PSN, as the SOE network is principally accessed via a computer. (Doc. 135 at 4:17-20.) However, certain SOE games can also be played through the PSN. (Id.) As of January 25, 2011, the PSN had over 69 million users worldwide and SOE had over 24.6 million users worldwide. (FACC ¶¶ 41, 43.)

5 Plaintiffs allege that all user Personal Information was stored and maintained by Sony in perpetuity, regardless of whether the user deactivates or terminates their account, and that Sony continually monitors and records users’ PSN activities, purchases, and usage. (FACC ¶¶ 50, 51.)
who established accounts with SOE had to agree to SOE’s User Agreement (“SOE User Agreement”) and SOE’s Privacy Policy (“SOE Privacy Policy”).  

On April 16, 2011 or April 17, 2011, Plaintiffs allege that hackers accessed Sony’s Network (computer systems, servers, and databases), thereby stealing the Personal Information of millions of Sony’s customers, including Plaintiffs.  

Plaintiffs further allege that even though Sony discovered that PSN and Qriocity user data had been stolen as early as April 17, 2011, Sony did not notify Plaintiffs and other affected consumers at that time.  

Instead, on April 20, 2011, Sony simply took the PSN and Qriocity systems offline, stating that “[w]e’re aware certain functions of PlayStation Network are down.  We will report back here as soon as we can with more information.”  

Thereafter, the PSN and Qriocity systems remained offline for almost a month while Sony conducted a system audit to determine the cause of the breach.  

During this time, Plaintiffs and the other Class members were unable to use Sony Online Services, and many were unable to access Third Party Services via their Consoles.  

Between April 21, 2011 and April 25, 2011, while Qriocity and the PSN remained offline, Plaintiffs allege that Sony continued to misrepresent the circumstances of the breach.  

Specifically, Plaintiffs allege that Sony did not inform the public of the breach until April 26, 2011, when Sony made a public statement that user Personal Information had been compromised, and encouraged those affected to “remain vigilant, to review [their] account statements[,] and to monitor [their] credit reports.”  

Shortly thereafter, Plaintiffs contend Sony admitted that its failures “may have had a financial impact on our loyal customers. We are currently reviewing options and will update you when the service is restored.”  

Plaintiffs further allege that Sony conceded that “[s]ome games may require access to PSN for trophy sync, security checks[,] or other network functionality[,] and therefore cannot be played offline.”  

On May 2, 2011, Sony also took SOE offline, and announced that SOE user Personal Information may have been compromised in the breach,
(Id. at ¶ 83). This was the first time SOE users were informed that their Personal
Information may have been compromised as a result of the intrusion. (Id. at ¶ 83.)

On April 30, 2011, ten days after Sony took the PSN and Qriocity systems offline,
Sony announced that it would compensate PSN and Qriocity users in the United States
with free identity theft protection services, certain free downloads and online services,
and would consider helping customers who had to apply for new credit cards. (Id. at ¶
85.) Likewise, on May 12, 2011, ten days after Sony took the SOE network offline,
Sony announced that it would compensate SOE users in the United States by offering
free identity theft protection services, one month of free service, and certain free in-game
bonuses and currency. (Id. at ¶ 86.)

II. Procedural History

On August 16, 2011, the Judicial Panel on Multidistrict Litigation transferred
certain civil actions from various district courts across the country into one consolidated
action before this Court. (Doc. No. 1.) On November 11, 2011, the Court appointed a
Liaison Counsel and a Plaintiffs’ Steering Committee (“PSC”) to streamline the process.
(Doc. No. 61.) On January 31, 2012, the PSC filed a Consolidated Class Action
Complaint (“Consolidated Complaint”), (Doc. No. 78), and on March 16, 2012, Sony
moved to dismiss the Consolidated Complaint, (Doc. No. 94). The Court heard oral
argument on the motion on September 27, 2012, and granted in part and denied in part
Sony’s motion to dismiss the Consolidated Complaint on October 11, 2012. (Doc. No.
120.) Plaintiffs filed the operative FACC on December 10, 2012. (Doc. No. 128.) The
FACC contains eleven named Plaintiffs from nine different states and alleges fifty-one
independent causes of action. (Id.)

III. Named Plaintiffs

Robert M. Bova (“Bova”) resides in Tewksbury, Massachusetts and alleges that he
acquired his PS3 in 2008. (FACC ¶ 18.) In or around 2009, Bova created a PSN

6 The FACC adds five additional named Plaintiffs and forty-four additional causes of action. (Compare Doc. No. 78 and Doc. No. 128.)
account and provided his Personal Information to Sony, including information possibly regarding his Bank of America Visa and TD Bank debit card accounts. (Id.) Bova used the PSN through his PS3 to play games and to download additional game content such as “map packs.” (Id.) As a result of the intrusion, Bova’s Personal Information was stolen, he was unable to access the PSN during the brief interruption in service, and he purchased credit monitoring services at a cost of approximately $10.00 per month. (Id.) Bova does not allege when he purchased credit monitoring services or that he experienced any unauthorized charges as a result of the intrusion. (Id.)

Christian Pierce Kalled (“Kalled”) resides in Wolfeboro, New Hampshire and alleges that he acquired his PS3 in 2009. (Id. at ¶ 19.) On or about October 21, 2009, Kalled created a PSN account and provided his Personal Information to Sony, including information possibly regarding his American Express credit card. (Id.) Kalled used the PSN through his PS3 to play games, to download game updates, to browse the Internet, and to stream prepaid media content from Netflix. (Id.) As a result of the intrusion, Kalled’s Personal Information was stolen, he was unable to access the PSN during the brief interruption in service, and he was unable to access his Netflix account through his PS3. (Id.) Kalled does not allege that he experienced any unauthorized charges on any of his accounts as a result of the intrusion. (Id.)

Scott Lieberman (“Lieberman”) resides in Plantation, Florida and alleges that he acquired his PS3 in early 2007. (Id. at ¶ 20.) In or around 2007, Lieberman created a PSN account and provided his Personal Information to Sony, including information regarding his American Express credit card. (Id.) Lieberman used the PSN through his PS3 to play games, to download games, and to stream prepaid media content from Netflix. (Id.) As a result of the intrusion, Lieberman’s Personal Information was stolen, he was unable to access the PSN during the brief interruption in service, and he was unable to access his Netflix account through his PS3. (Id.) Lieberman does not allege that he experienced any unauthorized charges on any of his accounts as a result of the intrusion. (Id.)
Kyle Johnson ("Johnson") resides in San Diego, California and alleges that he acquired his PS3 in 2007. (Id. at ¶ 21.) In or around 2007, Johnson created a PSN account and provided his Personal Information to Sony, including information regarding his Discover, American Express, and Visa credit card accounts. (Id.) Johnson used the PSN through his PS3 to play games, purchase and download games, and stream prepaid media content from Netflix. (Id.) As a result of the intrusion, Johnson’s Personal Information was stolen, he was unable to access the PSN during the brief interruption in service, and he was unable to access his Netflix account through his PS3. (Id.) In or around October 2011, Johnson alleges two unauthorized charges appeared on his Visa card. (Id.) Johnson does not allege whether these charges were later reimbursed. (Id.)

Arthur Howe ("Howe") resides in San Diego, California and alleges that he acquired his PS3 in 2008. (Id. at ¶ 22.) Howe alleges he created two PSN accounts, one for him and one for his minor son. (Id.) In order to register for both accounts, Howe alleges he provided his Personal Information to Sony, including his Union Bank debit/credit card account and a U.S. Bank account. (Id.) Howe used the PSN through his PS3 to play games, purchase and download games such as “map packs,” and stream prepaid media content from Netflix. (Id.) As a result of the intrusion, Howe’s Personal Information was stolen, he was unable to access the PSN during the brief interruption in service, and he was unable to access his Netflix account through his PS3. (Id.) Howe also alleges that he was forced to close two bank accounts and purchased credit monitoring services at a charge of approximately $9.00 per month. (Id.) Howe does not allege that he experienced any unauthorized charges on any of his accounts as a result of the intrusion, nor does Howe allege that he was forced to close his banks accounts due to unauthorized charges. (Id.)

Christopher Munsterman ("Munsterman") resides in Kansas City, Missouri and alleges that he acquired his PS3 in 2008. (Id. at ¶ 23.) In or around 2008, Munsterman created a PSN account and provided his Personal Information to Sony, including information possibly regarding his Commerce Visa Debit card. (Id.) Munsterman used
the PSN through his PS3 to play games, download games and movies, browse the
internet, and stream prepaid media content from Netflix. (Id.) As a result of the
intrusion, Munsterman’s Personal Information was stolen, he was unable to access the
PSN during the brief interruption in service, and he was unable to access his Netflix
account through his PS3. (Id.) Munsterman does not allege that he experienced any
unauthorized charges on any of his accounts as a result of the intrusion. (Id.)

Adam Schucher (“Schucher”) resides in Surfside, Florida and alleges that he
acquired his PS3 in mid-2008. (Id. at ¶ 24.) In or around 2008, Schucher created a PSN
account and provided his Personal Information to Sony, including information regarding
his Citibank Visa credit card. (Id.) Schucher used the PSN through his PS3 to purchase
and download karaoke songs for Karaoke Revolution Presents: American Idol. (Id.) As
a result of the intrusion, Schucher’s Personal Information was stolen and he was unable
to access the PSN during the brief interruption in service. (Id.) Schucher does not allege
that he experienced any unauthorized charges on any of his accounts as a result of the
intrusion. (Id.)

Rebecca Mitchell (“Mitchell”) resides in East Lansing, Michigan and alleges that
she acquired her PS3 in 2009. (Id. at ¶ 25.) In or around 2009, Mitchell created a PSN
account and provided her Personal Information to Sony, including information regarding
her mother’s credit card and her own Visa debit card. (Id.) Mitchell used the PSN to
play games and download karaoke songs for the PlayStation game Sing Star. (Id.) As a
result of the intrusion, Mitchell’s Personal Information was stolen and she was unable to
access the PSN during the brief interruption in service. (Id.) Mitchell does not allege
that she experienced any unauthorized charges on any of her accounts or her mother’s
accounts as a result of the intrusion. (Id.)

Christopher Wilson (“Wilson”) resides in Dallas, Texas and alleges that he
acquired his PS3 in January 2007. (Id. at ¶ 26.) In or around 2007, Wilson created a
PSN account and provided his Personal Information to Sony, including information
regarding his Chase Bank Visa debit card. (Id.) Wilson used the PSN to play games and
8
stream prepaid media content from Netflix. (Id.) As a result of the intrusion, Wilson’s Personal Information was stolen, and he was unable to access the PSN during the brief interruption in service. (Id.) Wilson does not allege that he experienced any unauthorized charges on any of his accounts as a result of the intrusion. (Id.)

James Wright (‘‘Wright’’) resides in Columbus, Ohio and alleges that he acquired his PS3 in 2008. (Id. at ¶ 27.) In or around 2008 or 2009, Wright created a SOE account, a Qriocity account, and PSN account, and provided his Personal Information to Sony, including information regarding his Visa US Bank debit/credit card (Id.) Wright used his SOE account to play DC Universe Online, his Qriocity account to play music, and his PSN account to play games and stream prepaid media content from Netflix. (Id.) As a result of the intrusion, Wright’s Personal Information was stolen and he was unable to access his SOE, Qriocity, and PSN accounts during the brief interruption in service. (Id.) Wright does not allege that he experienced any unauthorized charges on any of his accounts as a result of the intrusion. (Id.)

Timothy B. Whyland (‘‘Whyland’’) resides in Baldwinsville, New York and alleges that he acquired his PS3 in 2009. (Id. at 28.) In or around 2009, Whyland created a PSN account and provided his Personal Information to Sony, including information regarding his debit card. (Id.) Whyland used the PSN to play games and download additional golf courses for Tiger Woods Golf Masters PGA Tour 2012 and maps for Battlefield Bad Company 2. (Id.) As a result of the intrusion, Whyland’s Personal Information was stolen and he was unable to access his PSN for approximately twenty-one (21) days. (Id.) Whyland does not allege that he experienced any unauthorized charges on any of his accounts as a result of the intrusion. (Id.)

LEGAL STANDARDS

A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A motion to dismiss pursuant to Rule 12(b)(6) tests the legal sufficiency of the claims asserted in the complaint. Fed. R. Civ. P. 12(b)(6); Navarro v. Block, 250 F.3d 729, 731 (9th Cir. 2001). When ruling on a
motion to dismiss under Rule 12(b)(6), the court must accept all factual allegations pleaded in the complaint as true, and must construe them and draw all reasonable inferences from them in favor of the nonmoving party. *Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 337–38 (9th Cir.1996). In doing so however, the court is not bound to accept “legal conclusions” as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 664 (2009).

To avoid a Rule 12(b)(6) dismissal, a complaint need not contain detailed factual allegations; rather, the complaint must plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim has “facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id*. “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’ ” *Id.* (quoting *Twombly*, 550 U.S. at 557). As a result, it is not proper for the court to assume that “the [plaintiff] can prove facts that [he or she] has not alleged or that defendants have violated . . . laws in ways that have not been alleged.” *Associated Gen. Contractors of Cal., Inc. v. Cal. State Council of Carpenters*, 459 U.S. 519, 526 (1983).

Complaints alleging fraud must satisfy the heightened pleading requirements of Rule 9(b). Rule 9(b) requires that in all averments of fraud or mistake, the circumstances constituting that fraud or mistake should be stated with particularity. Malice, intent, knowledge, and other conditions of a person’s mind may be alleged generally. A pleading is sufficient under Rule 9(b) if it “state[s] the time, place[,] and specific content of the false representations as well as the identities of the parties to the misrepresentation.” *Misc. Serv. Workers, Drivers & Helpers v. Philco–Ford Corp.*, 661 F.2d 776, 782 (9th Cir. 1981) (citations omitted); see also *Vess v. Ciba–Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 2000)).
Regardless of the title given to a particular claim, allegations grounded in fraud are subject to Rule 9(b)’s pleading requirements. *Vess*, 317 F.3d at 1103-04; *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009); *Bros. v. Hewlett-Packard Co.*, No. C–06–02254 RMW, 2006 WL 3093685, at *7 (N.D. Cal. 2006).

In interpreting federal law, a transferee court in a multidistrict case should look to the law of its own circuit rather than the law of the transferor courts’ circuits. *In re Nat’l Century Fin. Enters., Inc., Inv. Litig.*, 323 F. Supp. 2d 861, 876–77 (S.D. Ohio 2004) (citing *In re Korean Air Lines Disaster of Sept. 1, 1983*, 829 F.2d 1171, 1176 (D.C. Cir. 1987)); *In re Methyl Tertiary Butyl Ether (“MTBE”) Prods. Liab. Litig.*, No. 00–1898, 2005 WL 106936, at *5 (S.D.N.Y. Jan. 18, 2005). Thus, although the parties have cited cases from various circuits discussing Rule 9(b)’s heightened pleading requirements, the Court will analyze federal procedural law in accordance with Ninth Circuit precedent.

**DISCUSSION**

The fifty-one claims alleged in the FACC can be categorized into nine sub-groups: (1) negligence; (2) negligent misrepresentation; (3) breach of express warranty; (4) breach of implied warranty; (5) unjust enrichment; (6) violation of state consumer protection statutes; (7) violation of the California Database Breach Act; (8) violation of the federal Fair Credit Reporting Act; and (9) partial performance/breach of the covenant of good faith and fair dealing. Sony moves to dismiss the FACC on the basis that Plaintiffs lack standing and that each cause of action fails to state a claim upon which relief can be granted. Each is discussed in turn.

**I. Standing**

Sony’s standing argument is two-fold. First, Sony contends SOE should be dismissed as a named Defendant because Plaintiffs do not have standing to pursue non-Ohio state law claims against SOE on behalf of non-Ohio residents. And second, Sony contends Plaintiffs’ amended allegations fail to establish Article III standing in light of the Supreme Court’s recent decision in *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013).
A. Standing to Assert Claims Against SOE

First, Sony contends Plaintiffs lack standing to pursue non-Ohio state-law claims on behalf of non-Ohio residents because Plaintiff Wright, an Ohio resident, is the only named Plaintiff that is an SOE network subscriber. Plaintiffs do not rebut that Wright is the only SOE network subscriber, but contend that Wright has standing to pursue claims: (1) on behalf of SOE network subscribers alleging violations of Ohio law; and (2) on behalf of all SOE network subscribers, regardless of their state of residence, for enforcement of the settlement agreement and alleged violations of the FCRA. The Court agrees. As stated below, although each of Plaintiffs’ claims under Ohio law and the FCRA are dismissed without leave to amend, Plaintiffs have standing to assert claims against SOE for enforcement of the settlement agreement and/or breach of the covenant of good faith and fair dealing. Accordingly, Sony’s motion to dismiss SOE as a named Defendant is DENIED.

B. Article III Standing

Second, in an argument relegated to a footnote, Sony contends the FACC should be dismissed for lack of Article III standing because Plaintiffs’ amended allegations have once again failed to allege an “injury-in-fact” as a result of the intrusion. (Doc. No. 135 at 9 n.12.) The Court’s prior order denied this exact argument, finding that under Krottner v. Starbucks, 628 F.3d 1139, 1142 (9th Cir. 2010), Plaintiffs had sufficiently alleged that their “sensitive Personal Information [was] wrongfully disseminated, thereby increasing the risk of future harm,” regardless of whether actual “harm [had] yet occurred.” (Doc. No. 120 at 13:17-19.) Sony now urges the Court to reconsider this ruling based on the Supreme Court’s recent decision in Clapper v. Amnesty International, 133 S. Ct. 1138 (2013). Because Article III standing is an “indispensable part of a plaintiff’s case,” and not merely a pleading requirement, the Court reconsiders its prior ruling. Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992).

To establish Article III standing, a plaintiff must plead: (1) injury-in-fact; (2) causation; and (3) redressability. Lujan, 504 U.S. at 560–61. The “injury-in-fact”
element requires a plaintiff to plead the “invasion of a legally protected interest which is 
(a) concrete and particularized, and (b) actual or imminent, not conjectural or hypotheti-
cal.” Id. (citations omitted). Analyzing the “injury-in-fact” requirement, the Supreme 
Court in Clapper considered whether the respondents, who alleged that their work 
required them to engage in sensitive international communications with individuals 
potentially targeted under the Foreign Intelligence Surveillance Act (the “Act”), had 
Article III standing to declare the Act unconstitutional and/or to obtain an injunction 
against surveillance authorized under the Act. 133 S. Ct. at 1142–43. Respondents 
argued that they had sufficiently alleged an “injury-in-fact” based on: (1) the objectively 
reasonable likelihood that their communications would at some point be targeted under 
the Act; and (2) the fact that they had already taken costly and burdensome measures to 
protect the confidentiality of their international sources. Id. at 1147–54.

The Supreme Court rejected both arguments. Id. With regard to the first argu-
ment, the Supreme Court stated that although it may be “objectively reasonable” that 
respondents’ communications may at some point be intercepted under the Act, respon-
dents had failed to show that the “threatened injury” was “certainly impending.” Id. at 
1147. The Supreme Court noted that a “speculative chain of possibilities . . . based on 
potential future surveillance” was not enough. Id. at 1150. With regard to respondents’ 
second argument, the Supreme Court stated that if parties could base Article III standing 
on reasonably incurred costs to avoid the risk of future harm, it would “water[] down the 
fundamental requirements of Article III.” Id. at 1151. “If the law were otherwise, an 
enterprising plaintiff would be able to secure a lower standard for Article III standing 
simply by making an expenditure based on a nonparanoid fear.” Id. Therefore, the 
Supreme Court held that even though respondents’ measures to avoid surveillance 
authorized under the Act was not “fanciful, paranoid, or otherwise unreasonable,” 
respondents could not “manufacture standing merely by inflicting harm on themselves 
based on fears of hypothetical harm that was not “certainly impending.” Id. at 1151.
Based on the above, Sony argues *Clapper* tightened the “injury-in-fact” analysis set forth by the Ninth Circuit in *Krottner v. Starbucks* and previously relied upon by the Court in its prior order. The Court does not agree. The Ninth Circuit in *Krottner* found Article III standing based on a “credible threat of harm” that was “both real and immediate, not conjectural or hypothetical,” 628 F.3d at 1143. In contrast, the Supreme Court in *Clapper* found that respondents failed to sufficiently allege Article III standing because a speculative chain of possibilities based on potential future surveillance was not enough to plausibly allege a “certainly impending” injury. 133 S. Ct. at 1150. Therefore, although the Supreme Court’s word choice in *Clapper* differed from the Ninth Circuit’s word choice in *Krottner*, stating that the harm must be “certainly impending,” rather than “real and immediate,” the Supreme Court’s decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court’s decision overrule previous precedent requiring that the harm be “real and immediate.” To the contrary, the Supreme Court’s decision in *Clapper* simply reiterated an already well-established framework for assessing whether a plaintiff had sufficiently alleged an “injury-in-fact” for purposes of establishing Article III standing. *Id.* at 1147 (“Thus, we have repeatedly reiterated that ‘threatened injury must be certainly impending to constitute injury in fact,’ and that ‘[a]llegations of possible future injury’ are not sufficient.”) (quoting *Whitmore v. Ark.*, 495 U.S. 149, 158 (1990)).

Therefore, the Court finds both *Clapper* and *Krottner* controlling, and case law in this circuit analyzing the “injury-in-fact” requirement following *Krottner* highly persuasive. For example, courts in this circuit have routinely denied motions to dismiss based on Article III standing where a plaintiff alleges that his personal information was collected and then wrongfully disclosed, as opposed to alleging that his personal

---

See also *Cent. Delta Water Agency v. United States*, 306 F.3d 938, 947–48 (9th Cir. 2002) (holding that “the possibility of future injury may be sufficient to confer standing on plaintiffs” and concluding that the suit could proceed when the plaintiffs demonstrated a factual issue about “whether they suffer a substantial risk of harm”).
Compare In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 711–12 (N.D. Cal. 2011) (finding plaintiffs’ allegations that their personal information was disclosed as opposed to just collected and retained by defendants sufficient for purposes of establishing Article III standing), Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102, 1108–09 (N.D. Cal. 2010) (finding plaintiffs’ allegations that their personal information was collected and then disclosed sufficient for purposes of establishing Article III standing), and San Luis & Delta-Mendota Water Auth. v. U.S. Dep’t of the Interior, 905 F. Supp. 2d 1158, 1171 (E.D. Cal. 2012) (“Although it was not guaranteed that reduced allocations would come to pass, the threat of harm was certainly real, not conjectural or hypothetical.”), with Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 WL 1282980, at *3 (N.D. Cal. Mar. 26, 2013) (“Yunker does not allege that he disclosed sensitive financial information, such as a social security number or a credit card number, to Pandora. Further, he has not alleged that anyone has breached Pandora’s servers.”), Low v. LinkedIn Corp., No. 11-cv-01468-LHK, 2011 WL 5509848, at *6 (N.D. Cal. Nov. 11, 2011) (distinguishing Krottner in that the plaintiff had not alleged that his highly personal information had been stolen and then exposed to the public), and In re Google, Inc. Privacy Policy Litig., No. C 12-01382 PSG, 2012 WL 6738343, at *6 (N.D. Cal. Dec. 28, 2012) (dismissing plaintiffs’ claims based on Google’s policy of retaining personal information for lack of Article III standing because there were no allegations plaintiffs’ personal information had been disseminated).

---

Although only persuasive, courts in other circuits have also held that a plaintiff can establish an “injury-in-fact” by alleging a threat of future harm. See, e.g., Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (stating that exposure to toxic substances creates a cognizable injury for standing purposes “even though exposure alone may not provide sufficient ground for a claim under state tort law”); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (holding that Article III standing was satisfied where a defective medical implement presented an increased risk of future health problems); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000) (en banc) (“Threats or increased risk thus constitutes cognizable harm.”); Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (“The injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant’s actions.”).
Therefore, the Court finds Plaintiffs’ allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion sufficient to establish Article III standing at this stage in the proceedings. (FACC ¶¶ 18-29, 119-123, 124-127.) Although Sony argues that Plaintiffs’ allegations are insufficient because none of the named Plaintiffs have alleged that their Personal Information was actually accessed by a third party, neither Krottner nor Clapper require such allegations. Instead, Plaintiffs have plausibly alleged a “credible threat” of impending harm based on the disclosure of their Personal Information following the intrusion.9 See Cherri v. Mueller, No. 12-11656, 2013 WL 2558207, at *9 (E.D. Mich. June 11, 2013) (stating that after Clapper, a plaintiff need only allege a “certainly impending injury that is fairly traceable to” the defendant’s purported conduct to withstand a motion to dismiss). Accordingly, the Court DENIES Sony’s motion to dismiss based on Article III standing.10

II. Failure to State a Claim Under Rule 12(b)(6)

A. Negligence Claims

Plaintiffs assert negligence claims under California law (Count 5), Florida law (Count 11), Massachusetts law (Count 14), Missouri law (Count 27), and Ohio law (Count 43). (FACC ¶¶ 196-211, 244-249, 262-270, 355-360, 451-456.) Each claim requires a plaintiff to allege the following four elements: (1) the existence of a legal

---

9 Krottner, 628 F.3d at 1143 (finding an “injury-in-fact” when plaintiffs pled an increased risk of harm following the theft of a laptop that contained their personal data); Doe 1, 719 F. Supp. 2d at 1109–11 (holding that plaintiffs were injured by defendant’s collection and publication of “highly sensitive personal information,” including credit card numbers, social security numbers, financial account numbers, and information regarding plaintiffs’ personal issues, including sexuality, mental illness, alcoholism, incest, rape, and domestic violence).

10 Notwithstanding controlling case law in this circuit, and the Court’s previous order, Sony again directs the Court to consider the Third Circuit’s reasoning in Reilly v. Ceridian Corporation, 664 F.3d 38 (3rd Cir. 2011), wherein the Third Circuit affirmed the trial court’s dismissal based on lack of Article III standing. Although the Court acknowledges the Third Circuit’s holding in Reilly, the Court once again reiterates that Reilly is only persuasive authority.
duty; (2) breach of that duty; (3) causation; and (4) cognizable injury. Sony moves to
dismiss each claim on the basis that Plaintiffs have failed to allege a cognizable injury,
and even if they had, Plaintiffs have failed to allege that Sony had a legal duty to
guarantee the security of Plaintiffs’ Personal Information. The Court first addresses the
Florida, Missouri, and Ohio negligence claims, and then addresses the California and
Massachusetts negligence claims. 12

1. Florida, Missouri, and Ohio Negligence Claims

The Florida, Missouri, and Ohio negligence claims contain identical factual
allegations. (FACC ¶¶ 244-249, 355-360, 451-456.) Each claim alleges that because
Sony requested, gathered, and promised to secure Plaintiffs’ Personal Information, Sony
had a duty to provide reasonable security consistent with industry standards, to ensure
Sony Online Services were secure, and to protect Plaintiffs’ Personal Information from
theft or misuse. Plaintiffs allege Sony breached this duty by failing to adequately secure
its network, and that Plaintiffs suffered “economic injury and property damage” as a
result of the intrusion. (Id. at ¶¶ 249, 360, 456.) The FACC does not explicitly allege
what economic injury and/or property damage Plaintiffs allegedly suffered as a result of
the intrusion.

Although Plaintiffs are not required to put forth evidence of their alleged injury at
this stage in the proceeding, Plaintiffs’ allegations of causation and harm are wholly
conclusory, and therefore fail to put the Court or Sony on notice of the specific relief
requested. Iqbal, 556 U.S. at 663 (“A claim has facial plausibility [under Rule 8] when
the pleaded factual content allows the court to draw the reasonable inference that the
defendant is liable for the misconduct alleged.”); In re Polyurethane Foam Antitrust

11 See, e.g., Paz v. Cal., 994 P.2d 975, 980–81 (Cal. 2001); Meyers v. City of
Jacksonville, 754 So. 2d 198, 202 (Fla. 2000); Jupin v. Kask, 849 N.E.2d 829, 834–35
(Mass. 2006); Am. Mortg. Inv. Co. v. Hardin-Stockton Corp., 671 S.W.2d 283, 292 (Mo.
1984); Mussivand v. David, 544 N.E.2d 265, 270 (Oh. 1989).

12 Neither party addressed the Court’s tentative ruling at oral argument, which
stated that each negligence claim was subject to dismissal without leave to amend based
on Plaintiffs’ failure to allege a cognizable injury and/or based on the economic loss
document.
Litig., 799 F. Supp. 2d 777, 792 (N.D. Ohio 2011), reconsideration denied (Sept. 15, 2011) (stating that conclusory allegations fail to put the defendant on notice of the claims alleged against it). For example, Plaintiffs do not specifically allege what economic injury they allegedly suffered as a result of Sony’s negligence, what property was allegedly damaged, or how the alleged property damage was proximately caused by Sony’s breach. Merely appending a clause incorporating by reference all prior allegations is insufficient, especially when Plaintiffs have alleged fifty-one independent causes of action in a complaint spanning over a hundred pages. See, e.g., Brandon v. City of N.Y., 705 F. Supp. 2d 261, 268–69 (S.D.N.Y. 2010) (“Such general allegations, without supporting facts other than a clause incorporating an entire complaint by reference, are insufficient to withstand even a motion to dismiss . . .”); Noel v. Bank of Am., No. 12-4019-SC, 2012 WL 5464608, at * 3 (N.D. Cal. Nov. 8, 2012) (stating that incorporation by reference language failed to meet Rule 8’s pleading requirements because the plaintiff failed to connect specific allegations to the elements of her claims.) It is the Plaintiffs’ burden—not the Court’s—to identify the specific relief sought for each individual cause of action.

Therefore, although the Florida, Missouri, and Ohio negligence claims were not previously dismissed for lack of specificity in the Consolidated Complaint, because these claims appeared for the first time in the FACC, the Court finds its previous order dismissing the California negligence claim sufficiently put Plaintiffs’ counsel on notice that conclusory allegations of causation and harm would not suffice. (Doc. No. 120 at 18-20.) This is especially true in light of Plaintiffs’ factual allegations with respect to the Massachusetts negligence claim, which also appeared for the first time in the FACC, as this claim includes specific allegations of causation and harm. As a result, the Court finds Plaintiffs’ counsel, who are sophisticated attorneys well versed in high-profile class-action litigation, were well aware of what was required to state a claim for negligence, and further amendment of these claims would prejudice Defendants. See Eminence Capital, LLC v. Aspeon, Inc., 316 F.3d 1048, 1052 (9th Cir. 2003) (“As this circuit
and others have held, it is the consideration of prejudice to the opposing party that carries the greatest weight.”). Accordingly, the Court GRANTS Sony’s motion to dismiss the Florida, Missouri, and Ohio negligence claims without leave to amend.

2. California and Massachusetts Negligence Claims

Similar to the Florida, Missouri, and Ohio negligence claims, the California and Massachusetts negligence claims contain identical factual allegations. ¹³ (FACC ¶¶ 196-211, 262-270.) Each claim alleges that Sony owed two independent legal duties that were separately breached: (1) the duty to timely disclose the nature of the intrusion, which was breached when Sony delayed in informing Plaintiffs that their Personal Information may have been disclosed to third parties; and (2) the duty to exercise reasonable care in safeguarding Plaintiffs’ Personal Information, which was breached when Sony failed to adopt, implement, and maintain adequate security measures to protect Plaintiffs’ Personal Information. (Id. at ¶¶ 197-200, 263-266.) As a result of Sony’s negligence, and with respect to the breach of both duties, Plaintiffs allege they incurred economic damages, including the cost to purchase credit monitoring services, loss of use and value of Sony Online Services, loss of use and value of Third Party Services, and a diminution in value of their Consoles. (Id. at ¶¶ 211, 270.) The Court separately addresses Plaintiffs’ allegations of duty and breach.

a. Cognizable Injuries Resulting From Sony’s Duty to Timely Disclose the Intrusion

Assuming without deciding that Sony owed Plaintiffs a legal duty to timely disclose the intrusion and the possibility that Plaintiffs’ Personal Information may have been disclosed, the Court finds Plaintiffs have failed to allege a single cognizable injury proximately caused by Sony’s resulting breach. See Held v. Bail, 547 N.E.2d 336, 337 (Mass. 1989); Dalkilic v. Titan Corp., 516 F. Supp. 2d 1177, 1190 (S.D. Cal. 2007).

Although Plaintiffs allege that Plaintiff Johnson received notification of the intrusion on

¹³ The California negligence claim also alleges a special relationship between Sony and the California Class. (FACC ¶¶ 204-210.)
April 27, 2013, approximately ten days after the intrusion, and that Plaintiff Howe received notification of the intrusion on April 28, 2013, approximately eleven days after the intrusion, neither of these allegations set forth a plausible claim that the alleged untimely disclosure, and not the intrusion itself, resulted in Johnson or Howe’s alleged injuries. (FACC ¶¶ 21, 22.) See Berardi v. Menicks, 164 N.E.2d 544, 546–47 (Mass. 1960) (“[I]t is not enough to show the mere possibility of a causal connection; the probability of such a connection must be shown”). The same is true with respect to Plaintiff Bova. Although Plaintiffs did not specify when Bova was notified of the intrusion, the Court infers that Bova had constructive notice of the PSN intrusion on April 26, 2011 (when Sony issued a public statement), and that Bova had constructive notice of the SOE intrusion on May 2, 2011 (when Sony posted a Customer Service Notification on SOE’s website). However, as with Johnson and Howe, Plaintiffs allegations do not set forth a plausible claim for relief on the basis that the delay, and not just the intrusion, caused Bova’s alleged injuries. (Id. at ¶¶ 78, 83.) This cannot be left to conjecture or speculation. See Twombly, 550 U.S. at 561.

Therefore, even though the Court finds Plaintiffs may have alleged a brief delay in the time period between the intrusion and when Sony notified consumers of the intrusion, the Court finds Plaintiffs have failed to allege that their injuries—credit monitoring services, loss of use and value of the PSN, loss of use and value of Third Party Services, and/or a diminution in value of their Consoles—were proximately caused by Sony’s alleged untimely delay. See Stollenwerk v. Tri-W. Health Care Alliance, 254 F. App’x 664, 668 (9th Cir. 2007) (“Here, however, proximate cause is supported not only by the temporal, but also by the logical, relationship between the two events.”); Jorgensen v. Mass. Port Auth., 905 F.2d 515, 524 (1st Cir. 1990) (stating that Massachusetts law requires that the defendant’s conduct be the “but-for cause” of the plaintiff’s injury).

14 Plaintiffs fail to allege when Howe or Bova purchased credit monitoring services, whether Howe and Bova were aware of Sony’s Welcome Back Package offering free credit monitoring services, or whether Howe and Bova purchased credit monitoring services on account of Sony’s alleged untimely delay.
Accordingly, the Court GRANTS Sony’s motion to dismiss the California and Massachusetts negligence claims based on Sony’s alleged breach of the duty to timely disclose the nature of the intrusion. Because the Court finds further amendment of this claim would be futile, the Court grants Sony’s motion without leave to amend.

b. Cognizable Injuries Flowing From Sony’s Duty to Provide Reasonable Network Security

As set forth above, the FACC also alleges that Sony owed Plaintiffs Johnson, Howe, and Bova a duty to exercise reasonable care in safeguarding and protecting their Personal Information. (FACC ¶¶ 197, 263.) Plaintiffs allege this duty included, among other things, the duty to design, implement, maintain, and test Sony’s security system in order to ensure Plaintiffs’ Personal Information was adequately secured and protected. (Id.) Plaintiffs allege Sony breached this duty by failing to implement proper procedures to protect Plaintiffs’ Personal Information, and as a result, Plaintiffs incurred economic damages, including the cost to purchase credit monitoring services, loss of use and value of Sony Online Services, loss of use and value of Third Party Services, and/or a diminution in value of their Consoles. Sony moves to dismiss these claims on the basis that Plaintiffs have failed to allege: (1) a legal duty to provide reasonable security; and (2) cognizable injuries not barred by the economic loss doctrine. The Court discusses each in turn.

i. Legal Duty to Provide Reasonable Security

Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer’s confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. See, e.g., Witriol v. LexisNexis Grp., No. C05-02392 MJJ, 2006 WL 4725713, at *8 (N.D. Cal. Feb. 10, 2006); CUMIS Ins. Soc’y., Inc. v. BJ’s Wholesale Club, Inc., No. 051158, 2005 WL 6075375, at *4 (Mass. Super. Dec. 7, 2005) aff’d, 918 N.E.2d 36 (Mass. 2009); Yakubowicz v. Paramount Pictures Corp., 536 N.E.2d 1067, 1070 (Mass. 1989) (“A basic principle of negligence law is that
ordinarily everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm.”). As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.

ii. Economic Loss Doctrine

However, the existence of a legal duty and a corresponding breach are not the only elements required to state a claim for negligence—Plaintiffs must also allege appreciable, non-speculative harm proximately caused by Sony’s breach. See, e.g., Vinci v. Byers, 837 N.E.2d 1140, 1145 (Mass. App. Ct. 2005) (stating that appreciable harm is “injury, loss, or detriment that is capable of being measures or perceived”) (internal citations and quotations omitted); Int’l Engine Parts, Inc. v. Feddersen & Co., 9 Cal. 4th 606, 614 (Cal. 1995) (stating that a negligence claim requires appreciable, non-speculative, present injury). Here, Plaintiffs allege the following cognizable injuries resulted from Sony’s alleged breach: (1) expenses incurred to purchase credit monitoring services (Howe and Bova); (2) loss of use and value of Sony Online Services (Howe, Johnson, Bova); (3) loss of use and value of Third Party Services (Johnson and Howe); and (4) a diminution in value of Plaintiffs’ Consoles (Johnson, Howe, Bova). 15 (FACC ¶¶ 207, 211, 270.) Sony contends each of these injuries are barred by the economic loss doctrine as articulated under Massachusetts and California law.

Massachusetts generally prohibits the recovery of purely economic losses in tort absent personal injury or property damage. Aldrich v. ADD Inc., 770 N.E.2d 447, 454–55 (Mass. 2002). 16 Although there are exceptions to this general rule, which allow a

15 Although Paragraph 270 alleges Bova suffered a cognizable injury in the form of loss of use and value of Third Party Services, Paragraph 18 does not allege Bova subscribed to and/or accessed any Third Party Services via Sony Online Services.

16 The rationale behind the doctrine is that a “commercial user can protect himself by seeking express contractual assurances concerning the product (and thereby perhaps paying more for the product) or by obtaining insurance against losses.” Bay State–Spray

Similarly, under California law, “[i]n the absence of (1) personal injury, (2) physical damage to property, (3) a ‘special relationship’ existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed.” Kalitta Air, LLC v. Cent. Tex. Airborne Sys., Inc., 315 F. App’x 603, 605 (9th Cir. 2008) (quoting J’Aire Corp. v. Gregory, 598 P.2d 60, 62–63 (Cal. 1979) (setting forth the factors a court must consider when determining whether a special relationship exists between the parties). Put simply, the economic loss doctrine was created to prevent “the law of contract and the law of tort from dissolving one into the other.” Robinson Helicopter Co. v. Dana Corp., 34 Cal. 4th 979, 988 (Cal. 2004) (internal quotations omitted).

Based on the above, Sony moves to dismiss the California negligence claim on the basis that neither Howe nor Johnson have alleged personal injury or property damage as a result of the intrusion, nor have Howe or Johnson alleged a “special relationship” with & Provincetown S.S., Inc. v. Caterpillar Tractor Co., 533 N.E.2d 1350, 1354–55 (Mass. 1989).
Sony based on the factors articulated by the California Supreme Court in *J'Aire Corp. v. Gregory*, 598 P.2d 60 (Cal. 1979). Moreover, even if Plaintiffs could satisfy the *J'Aire* special relationship test, Sony contends the *J'Aire* factors are inapplicable because the duty Sony allegedly violated was specifically referenced in the PSN User Agreement, and therefore, can only form the basis of a contract claim. As a result, Sony contends Plaintiffs’ California negligence claim is nothing more than an attempt to plead around their contract with Sony, which clearly disclaims the economic losses Plaintiffs now seek to recover. Although Plaintiffs Johnson and Howe seemingly concede that the California negligence claim seeks to recover purely economic losses—credit monitoring fees, loss of use and value of the PSN, loss of use and value of Third Party Services, and a diminution in value of their Consoles—they nonetheless argue that they can recover these losses based on the *J'Aire* “special relationship” exception.

Before turning to the application of the *J'Aire* factors, the Court dispels Sony’s contention that their contract with Plaintiffs forecloses tort liability. As stated by the California Supreme Court in *Aas v. Superior Court*, “[a] person may not ordinarily recover in tort for the breach of duties that merely restate contractual obligations.” 24 Cal. 4th 627, 643 (Cal. 2004) (superseded by statute on other grounds) (quoting *Freeman & Mills, Inc. v. Belcher Oil Co.*, 11 Cal. 4th 85, 107 (Cal. 1995)). Based on this general rule, “courts will generally enforce the breach of a contractual promise through contract law, except when the actions that constitute the breach violate a social policy that merits the imposition of tort remedies.” *Id.* As a result, although a plaintiff will not be able to recover in tort based solely on allegations that a contract was negligently performed, a plaintiff may be able to pursue both contract and tort remedies if the plaintiff alleges that the contractual breach also violated “a duty independent of the contract arising from principles of tort law.” *Aas*, 24 Cal. 4th at 643; see also *Erlich v. Menezes*, 21 Cal. 4th 543, 550 (Cal. 1999). Accordingly, because Sony owed Plaintiffs a legal duty to provide reasonable network security (as articulated by the Court above), which was separate and independent from the PSN User Agreement, the Court finds Plaintiffs may pursue both
contract and tort remedies, to the extent Plaintiffs’ tort claims are not barred by the economic loss doctrine.\textsuperscript{17}

Under \textit{J’Aire} special relationship exception to the economic loss doctrine, the existence of a “special relationship” is based on a determination of the following six factors:

(1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant’s conduct and the injury suffered, (5) the moral blame attached to the defendant’s conduct and (6) the policy of preventing future harm.

\textit{J’Aire}, 598 P.2d at 63. All six factors must be considered by the court and the presence or absence of one factor is not decisive. \textit{Kalitta Air}, 315 F. App’x at 605–06.

Here, Plaintiffs Johnson and Howe allege a “special relationship” between the parties because: (1) Sony developed Sony Online Services for use with PSPs and PS3s and intended its contract with consumers, which required consumers to provide their Personal Information before registering for such services, to effect Plaintiffs and other class members; (2) if Sony did not reasonably perform its contractual obligations, in light of previous instances of admitted security vulnerabilities, Plaintiffs’ Personal Information could be disclosed; (3) Plaintiffs suffered injury as a result of the intrusion, including expenses incurred to purchase credit monitoring services, loss of use and value of Sony Online Services, loss of use of Third Party Services, and a diminution in value of their Consoles; (4) the injuries were a direct result of Sony’s lack of adequate, reasonable, and industry-standard security measures; (5) Sony’s conduct warrants moral blame because Sony promised to secure Plaintiffs’ Personal Information; and (6) holding Sony accountable will require Sony and other companies to provide reasonable, adequate, and industry-standard security measures. (FACC ¶¶ 204-211.)

After considering the six \textit{J’Aire} factors in light of Plaintiffs’ factual allegations, the Court finds Plaintiffs have failed to allege a “special relationship” with Sony beyond

\textsuperscript{17} The Court only addresses the \textit{J’Aire} exception because this was the only exception cited by Plaintiffs.
those envisioned in everyday consumer transactions, and therefore, negligence is the
correct legal theory on which to pursue recovery for Plaintiffs’ economic losses. See
2008) (“[W]e conclude, as a matter of law, that Midtec did not have a special relation-
ship with Greystone sufficient to support a negligence cause of action for economic
losses pursuant to J'Aire.”). The Court first addresses the degree of certainty that Sony’s
conduct proximately caused: (1) a loss of use and value of Sony Online Services and a
loss of use and value of Third Party Services; (2) costs incurred to purchase credit
monitoring services; and (3) a diminution in value of Plaintiffs’ Consoles. See Aas, 24
Cal. 4th at 646 (“Lacking that fundamental prerequisite to a tort claim, it is difficult to
imagine what other factors, singly or in combination, might justify the court in finding
liability.”).

First, with respect to the alleged loss of use and value of Sony Online Services and
the alleged loss of use and value of Third Party Services, neither are recoverable in
negligence because they were not proximately caused by Sony’s alleged failure to
provide reasonable network security and/or did not result in a measurable loss. Although
the amount of recoverable damages is usually a question of fact, which is a determination
not properly before the court on a motion to dismiss, the measure of damages, existence
of damages, and whether a plaintiff has sufficiently pled a causal connection between the
damage and the alleged harm is a question of law. See, e.g., Hendricks v. DSW Shoe
v. Whiting-Turner Contracting Co., 946 F.2d 1003, 1009 (2d Cir. 1991); Phillips v. TLC
Plumbing, Inc., 172 Cal. App. 4th 1133, 1139 (Cal. Ct. App. 2009); Berardi v. Menicks,
164 N.E.2d 544, 546–47 (Mass. 1960) (stating that “it is not enough to show the mere
possibility of a causal connection; the probability of such a connection must be shown”).
Therefore, because Plaintiffs acknowledge that Sony did not owe Plaintiffs a legal duty
to provide uninterrupted PSN service, it is nonsensical, and defies the bounds of
common sense for Plaintiffs to simultaneously seek damages for an interruption in PSN
service. (Doc. No. 146 at 33-34.) This disconnect in Plaintiffs’ factual allegations is additionally supported by Plaintiffs’ concession that access to the PSN is free, that Plaintiffs did not purchase premium PSN services, that Plaintiffs could access Third Party Services through other mediums, and that Sony’s disclaimed any right to uninterrupted PSN access. *See Grawitch v. Charter Commc’ns, Inc.*, No. 4:12CV01990 AGF, 2013 WL 253534, at *3 (E.D. Mo. Jan. 23, 2013) (finding the plaintiff had failed to state a pecuniary loss because “the upgraded service was provided for free and not at an increased cost”). Therefore, the Court finds neither of these damages were a foreseeable result of Sony’s alleged breach.

Second, with respect to Howe’s ability to recover costs incurred to purchase credit monitoring services, the Court finds Howe has failed to allege why these prophylactic costs were reasonably necessary, and therefore proximately caused by Sony’s alleged breach.¹⁸ In assessing whether credit monitoring services in the context of data breach cases are recoverable in negligence, courts have generally analogized to medical monitoring cases, which require a plaintiff to plead that the monitoring costs were both reasonable and necessary.¹⁹ *See Stollenwerk, 254 F. App’x at 666; Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 639 (7th Cir. 2007).* As a result, courts assessing data breach cases have found that where a state allows recovery for medical monitoring damages (as does California), and a plaintiff has sufficiently alleged a threat of identity theft (i.e., the opening of unauthorized accounts), a plaintiff may seek to recover expenses to purchase credit monitoring services. However, as with the recovery of medical monitoring costs, this is a high burden and requires a plaintiff to plead both a logical and temporal

---

¹⁸ Plaintiff Johnson does not allege he purchased credit monitoring services.

¹⁹ “Under the medical monitoring cases, individuals who have been exposed to potentially harmful substances but have no presently detectable illnesses may recover the costs of future medical surveillance by showing ‘through reliable expert testimony,’ (1) the ‘significance and extent of exposure,’ (2) the ‘toxicity of [the contaminant], [and] the seriousness of the [harm] . . . for which the individuals are at risk,’ and (3) the ‘relative increase in the chance of . . . [the harm] in those exposed,’ such that (4) ‘monitor[ing] the effects of exposure . . . is reasonable and necessary.’” *Stollenwerk, 254 F. App’x at 666* (quoting *Burns v. Jaquays Mining Corp.*, 752 P.2d 28, 33 (Ariz. Ct. App. 1987)).
connection between the decision to purchase credit monitoring services and the defendant’s alleged breach. See Stollenwerk, 254 F. App’x 664 at 668; Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 915 (N.D. Cal. 2009) aff’d, 380 F. App’x 689 (9th Cir. 2010) (“Ruiz cannot meet California’s standard for recovery of monitoring costs because he has presented no evidence that there was a significant exposure of his personal information, and he has presented no evidence that he has become a victim of identity theft.”).

Here, Plaintiff Howe has not met this high burden because has not alleged any instances of identity theft resulting from the intrusion. See Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 709 (S.D. Oh. 2007) (stating that the recovery of credit monitoring services as a measure of cognizable damages is a question of law to be decided by the court). Although Howe alleges that he was forced to close two bank accounts, Howe does not allege when he closed these accounts, why he closed these accounts, or whether he has ever been a victim of identity theft in the past. (FACC ¶ 22.) These allegations remain unchanged even though Plaintiffs were permitted leave to amend the Consolidated Complaint after Sony’s initial motion to dismiss. Therefore, in accordance with analogous medical monitoring cases and data breach cases from other districts, the Court finds Howe has failed to allege that his prophylactic credit monitoring costs were a reasonable foreseeable result of Sony’s alleged breach. 20

20 See, e.g., Kahle, 486 F. Supp. 2d at 713 (stating that “without direct evidence that the information was accessed or specific evidence of identity fraud” credit monitoring costs are not recoverable in negligence); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006) (granting summary judgment for the defendant because the plaintiff failed to establish the damages element, stating that credit monitoring fees in the absence of a present threat of identity theft did not suffice); Shafran v. Harley-Davidson, Inc., No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008) (“Courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy.”); Resnick v. AvMed, Inc., 693 F.3d 1317, 1326 (11th Cir. 2012) (finding that the plaintiffs’ allegations of identify theft crossed the line from “possible to probable” because the plaintiffs alleged that prior to the data breach they had never experienced any instances of identity theft, and always took the utmost precautions to keep their confidential information private); Pinero v. Jackson Hewitt Tax Serv. Inc., 594 F. Supp. 2d 710, 718 (E.D. La. 2009) (“Numerous courts have held that expenses related to credit monitoring to guard against future identity theft are not compensable damages.”); Giordano v. Wachovia Sec., LLC, No. 06-476 JBS, 2006 WL 2177036, at *3 (D.N.J. July 31, 2006) (“In all three cases, the district courts have held that, because the plaintiff’s injuries were solely the result of a perceived risk of future
Third, with respect to damages relating to an alleged diminution in value of
Plaintiffs’ Consoles, Plaintiffs have once again failed to allege enough facts for the Court
to adequately access the plausibility of the claim. See Balistreri v. Pacifica Police Dep’t,
901 F.2d 696, 699 (9th Cir. 1988) (stating that dismissal can be based on the lack of a
cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal
theory). As stated in the Court’s prior order, without allegations that Plaintiffs are using
their Consoles less as a result of the intrusion, or have reported problems with their
Consoles after the intrusion, Plaintiffs’ allegations of diminution in value fail to allege
how Plaintiffs have suffered an appreciable, non-speculative harm. See Aguilera v.
Pirelli Armstrong Tire Corp., 223 F.3d 1010, 1015 (9th Cir. 2000). Although the FACC
attempts to bolster the allegations in the Consolidated Complaint by alleging that
Plaintiffs’ Consoles diminished in value as a result of Sony’s failure to secure their
Personal Information and/or the brief interruption in PSN access, none of these addi-
tional allegations support a claim that is “plausible on its face.” Bell Atl. Corp. v.
Twombly, 550 U.S. 544, 547 (2007). As stated by countless courts considering this
issue, subjective allegations that a product has diminished in value are insufficient. See,
e.g, Arcand v. Brother Int'l Corp., 673 F. Supp. 2d 282, 301 (D.N.J. 2009) (“In evaluat-
ing whether a plaintiff has suffered an ascertainable loss, the Court need not countenance
‘hypothetical or illusory’ losses or the wholly subjective expectations of a consumer.”);
See In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012)
(“Purely economic damages to a plaintiff which stem from disappointed expectations
from a commercial transaction must be addressed through contract law; negligence is not
a viable cause of action for such claims.”).
Therefore, at this stage in the proceedings, although Plaintiffs are not required to come forward with evidence to support their allegations, Plaintiffs must set forth a plausible claim for relief. Plaintiffs have not done that here. See In re iPhone Application Litig., 844 F. Supp. 2d at 1064 (“All of the allegations of harm identified in the Amended Consolidated Complaint are either too speculative to support a claim for negligence under California law, or they stem from disappointed expectations from a commercial transaction and thus do not form the basis of a negligence claim.”). Instead, after over two years of motion practice conducted by highly sophisticated counsel, Plaintiffs have alleged nothing more than economic damages relating to “disappointed expectations from a commercial transaction,” all of which “must be addressed through contract law.” Id. “[N]egligence is not a viable cause of action for such claims,” and the Court will not allow expensive, potentially burdensome class action discovery to ensue in the absence of a viable cause of action. See Twombly, 550 U.S. at 558 (deficiencies in the complaint “should be exposed at the point of minimum expenditure of time and money by the parties and the court” given the prospect of costly discovery); Grigsby v. Valve Corp., No. C12-0553JLR, 2012 WL 5993755, at *4–6 (W.D. Wash. Nov. 14, 2012) (stating that the Twombly pleading standard is particularly demanding in “complex, large-scale” data breach class action litigation). Accordingly, the Court finds the third J’Aire factor weighs against finding a special relationship between the parties.

Plaintiffs’ allegations with respect to the remaining J’Aire factors fare no better. With regard to the first factor, the extent to which the transaction was intended to affect the plaintiff, the Court finds Plaintiffs have failed to allege why the transactions at issue were intended to affect Plaintiffs “in a way particular to [them], as opposed to all potential” consumers. Greystone Homes, 168 Cal. App. 4th at 1231 (stating that the “J’Aire test was not met because the sink sales at issue were like any other sink sale made by the product manufacturer—i.e., the product manufacturer had not specially made the sink for the benefit of the [plaintiffs]”). Therefore, as noted by countless California courts applying J’Aire, “[i]f a duty of care to avoid economic injury existed
[in every contract], every manufacturer would become an insurer, potentially forever, against economic loss from negligent defects in a product used for its intended purpose.”

Fieldstone Co. v. Briggs Plumbing Prods., Inc., 54 Cal. App. 4th 357, 368–69 (Cal. Ct. App. 1997); see also Ott v. Alfa-Laval Agri, Inc., 31 Cal. App. 4th 1439, 1455 (Cal. Ct. App. 1995) (“First, neither the pleadings nor the evidence suggests the 1970 milking system was ‘intended to affect’ the plaintiffs in any way particular to the plaintiffs, as opposed to all potential purchasers of the equipment.”); Greystone, 168 Cal. App. 4th at 1230–31. Therefore, because Plaintiffs have failed to allege that Sony developed the goods and services at issue for Plaintiffs’ specific benefit, above and beyond what was offered to all consumers, the Court finds this factor weighs against imposing a special relationship between the parties.

With regard to the second factor, the foreseeability of harm, the Court finds, as it did above, that Plaintiffs’ injuries were not a foreseeable result of Sony’s alleged negligence. As to the fourth factor, the closeness of the connection between the defendant’s conduct and the injury suffered, the Court finds Plaintiffs have sufficiently alleged a connection between Sony’s conduct and the brief interruption in PSN access. Finally, with regard to fifth and sixth factors, the moral blame attached to Sony’s conduct and the policy of preventing future harm, the Court finds Plaintiffs have alleged that Sony knew of its security vulnerabilities and that imposing liability might influence other businesses to take the necessary precautions. Thus, these factors also weigh in favor of Plaintiffs.

However, after collectively considering the J’Aire factors, the Court finds Plaintiffs have failed to allege a “special relationship” that would allow Plaintiffs to recover purely economic losses unaccompanied by physical injury or property damage. See, e.g., Carrau v. Marvin Lumber and Cedar Co., 93 Cal. App. 4th 281, 295 (2001) (barring recovery for the diminished value of a house in which defective windows were installed under the economic loss rule); Anthony v. Kelsey-Hayes Co., 25 Cal. App. 3d 442, 446 (Cal. Ct. App. 1972) (denying loss of bargain damages in negligence).

Accordingly, the Court GRANTS Sony’s motion to dismiss the California negligence
claims based on the economic loss doctrine without leave to amend. See *Leadsinger, Inc. v. BMG Music Pub.*, 512 F.3d 522, 532 (9th Cir. 2008).

**B. Negligent Misrepresentation /Innocent Misrepresentation/Negligent Omission**

Plaintiffs assert negligent misrepresentation claims under Florida law (Count 9), Massachusetts law (Count 15), Michigan law (Count 19), New Hampshire law (Count 31), Ohio law (Count 42), and Texas law (Count 47), an innocent misrepresentation claim under Michigan law (Count 20), and a negligent omission claim under Missouri law (Count 26). (FACC ¶¶ 234-238, 271-275, 300-304, 305-309, 346-354, 383-387, 446-450, 479-483.) Although there are slight differences between the required elements for each claim, each claim essentially requires Plaintiffs to allege that: (1) they relied upon a material misrepresentation made by Sony; and (2) that the misrepresentation resulted in a subsequent pecuniary loss.21 Sony contends Plaintiffs have failed in both respects, and independently moves to dismiss the Ohio negligent misrepresentation claim and the Missouri negligent omission claim. The Court first addresses Sony’s individual grounds for dismissing the Ohio and Missouri claims, and then addresses Sony’s global arguments for dismissing the remaining negligent misrepresentation claims.22

1. Ohio and Missouri Claims

First, Sony contends the Ohio negligent misrepresentation claim should be dismissed because Ohio only recognizes the claim if the alleged misrepresentation was


22 Neither party addressed the Court’s tentative ruling at oral argument, which stated that each of the misrepresentation and omission claims were subject to dismissal without leave to amend based on Plaintiffs failure to allege a cognizable injury and/or because the Ohio claim does not apply to consumer transactions. (Doc. No. 157.)
made for the guidance of others in the course of a business transaction. To support this contention, Sony relies on *Doe v. SexSearch.com* and *Thornton v. State Farm Mutual Auto Insurance Company*. Although Plaintiffs attempt to distinguish *Doe* and *Thornton*, Plaintiffs fail to cite any case law to the contrary and the Court finds their attempts only bolster Sony’s contentions.

   Under Ohio law, a “defendant is liable for negligent misrepresentation if he: (1) supplies false information (2) for the guidance of others in their business transaction (3) causing pecuniary loss to the plaintiff (4) while the plaintiff justifiably relied upon the information and (5) the defendant failed to exercise reasonable care or competence in obtaining or communicating the information.” *Doe*, 551 F.3d at 418. Here, Plaintiffs fail to satisfy the second element. As set forth in the FACC, Plaintiff Wright alleges that he registered for the PSN and SOE networks to play games and stream prepaid media from Netflix, both of which were presumably for personal and not business purposes. *See, e.g., Andersons, Inc. v. Consol, Inc.*, 348 F.3d 496, 505 (6th Cir. 2003) (acknowledging the distinct nature of a negligent misrepresentation claim under Ohio law); *Thornton*, 2006 WL 3359448, at *16 (“The Ohio Supreme Court is unequivocal that negligent misrepresentation is a business tort related to professional malpractice.”). Accordingly, because Plaintiffs do not allege that Wright registered for the PSN or SOE networks for business purposes, the Court GRANTS Sony’s motion to dismiss the Ohio negligent misrepresentation claim without leave to amend.

   Second, citing *Moore v. U.S. Bank* and *Lowdermilk v. Vescovo Building & Realty Company*, Sony contends the Missouri negligent omission claim should be dismissed because Missouri does not recognize such a claim. Although Plaintiffs do not offer an

---


opposition to Sony’s contentions, possibly because Sony’s arguments were relegated to a footnote, the Court finds further briefing on the issue unnecessary. Missouri does not recognize a separate cause of action for negligent omission; rather a plaintiff may plead omissions as the basis for a negligence claim. See, e.g., Govero v. Standard Oil Co., 192 F.2d 962, 964 (8th Cir. 1951); City of Kennett v. Wartsila N. Am., Inc., No. 4:05CV114 HEA, 2005 WL 3274334, at *3 (E.D. Mo. Dec. 2, 2005). Accordingly, the Court \textbf{GRANTS} Sony’s motion to dismiss the Missouri negligent omission claim without leave to amend. See In re Gen. Motors Corp. Anti-Lock Brake Prods. Liab. Litig., 174 F.R.D. 444, 446 (E.D. Mo. 1997) \textit{aff'd sub nom. Briehl v. Gen. Motors Corp.}, 172 F.3d 623 (8th Cir. 1999) (stating that a court does not “abuse its discretion in refusing to allow amendment of pleadings to change the theory of a case if . . . no valid reason is shown for the failure to present the new theory at an earlier time”).

\section{2. Remaining Negligent Misrepresentation Claims}

In addition to the arguments set forth above, Sony contends the remaining misrepresentation claims should be dismissed because Plaintiffs have failed to: (1) specify the actual misrepresentations upon which they relied; and (2) allege a pecuniary loss resulting from Plaintiffs’ reliance on the actionable misrepresentation. To the extent the Court finds Plaintiffs have sufficiently stated a claim, Sony also contends that the Michigan, New Hampshire, and Texas misrepresentation claims are barred by the economic loss doctrine.

\textbf{a. Actual Misrepresentations}

First, Sony contends the Florida, Massachusetts, Michigan, New Hampshire, and Texas misrepresentation claims should be dismissed because Plaintiffs have failed to allege actionable misrepresentations in compliance with Rule 9(b). Specifically, Sony argues the Florida, Massachusetts, and Texas claims should be dismissed because Plaintiffs have failed to identify what “advertising, packaging, and correspondence” the alleged misrepresentations were contained in, and the Florida and Texas claims should be dismissed because Plaintiffs have failed to identify how the alleged misrepresenta-
tions were “reiterated and disseminated by the officers, agents, representatives, servants, or employees of Defendants acting within the scope of their authority.” (FACC ¶¶ 232, 272, 384, 480, 235, 480.)

Although Sony raises valid arguments, the Court finds Plaintiffs have sufficiently alleged the specific representations they contend were false and/or misleading when made (representations regarding reasonable security and industry-standard encryption), and that these representations were contained in the PSN and SOE User Agreements and/or Privacy Policies, both of which were presented to Plaintiffs at the time they registered for the PSN or SOE network. Therefore, Plaintiffs have sufficiently alleged actionable misrepresentations in compliance with Rule 9(b). However, Plaintiffs’ allegations regarding the dissemination of these alleged misrepresentations by the officers, employees, and/or representatives of Sony do not satisfy Rule 9(b). Neither the FACC nor Plaintiffs’ opposition supports these allegations with the required specificity. Swartz v. KPMG LLP, 476 F.3d 756, 764–65 (9th Cir. 2007) (“Rule 9(b) does not allow a complaint to merely lump multiple defendants together but ‘require[s] plaintiffs to differentiate their allegations when suing more than one defendant . . . and inform each defendant separately of the allegations surrounding his alleged participation in the fraud.’”) (citing Haskin v. R.J. Reynolds Tobacco Co., 995 F. Supp. 1437, 1439 (M.D. Fla. 1998)). Accordingly, the Court finds Plaintiffs have sufficiently alleged actionable misrepresentations in compliance with Rule 9(b), but have failed to sufficiently allege how these misrepresentations were “reiterated and disseminated by the officers, agents, representatives, servants, or employees of Defendants acting within the scope of their authority.”

b. **Pecuniary Loss Flowing From Plaintiffs’ Reliance on the Alleged Misrepresentations**

Sony also contends that Plaintiffs have failed to allege a pecuniary loss flowing from the alleged negligent misrepresentations. The Court agrees. First, with respect to the Florida and Michigan negligent misrepresentation claims, Plaintiffs allege they
would not have registered with Sony Online Services or sent their Personal Information
to Sony had they known the truth regarding Sony’s network security. (FACC ¶¶ 234-
238, 300-304.) However, as stated above, because Plaintiffs’ Personal Information does
not have independent monetary value, registration and use of Sony Online Services was
provided to consumers free of charge, and none of the Plaintiffs allege that they paid for
premium PSN services, the Court finds Plaintiffs have failed to allege a pecuniary loss
caused by Sony’s alleged misrepresentations. See Doe v. Chao, 540 U.S. 614, 625
(2004) (finding that a plaintiff must allege an “actual, quantifiable, pecuniary loss” to
state a cause of action in tort); In Burrows v. Purchasing Power, LLC, No.
does not have an apparent monetary value that fluctuates like the price of goods or
services.”); Sipes v. Kinetra, LLC, 137 F. Supp. 2d 901, 910 (E.D. Mich. 2001) (requir-
ing a resulting damage to the plaintiff). Accordingly, the Court finds the Florida and
Michigan negligent misrepresentation claims fail to allege a pecuniary loss.

The same is true with respect to the Massachusetts, New Hampshire, and Texas
negligent misrepresentations claims and the Michigan innocent misrepresentation claim.
(FACC ¶¶ 271-275, 305-309, 383-387, 446-450.) Each claim alleges that Plaintiffs
would not have purchased their Consoles, Sony Online Services, and/or registered for
Sony Online Services, or paid as much for these products or services, had they known
the truth regarding Sony’s network security. However, as set forth above, Sony Online
Services was provided free of charge, and none of the Plaintiffs allege they paid for
premium PSN services. Moreover, and even more detrimental to Plaintiffs’ claims,
although Plaintiffs allege that they would not have purchased their Consoles “but for”
Sony’s alleged misrepresentations, Plaintiffs concede that they base their misrepresenta-
tion claims on statements contained in the PSN User Agreement and/or the PSN Privacy
Policy, both of which were presented to Plaintiffs “after” they purchased their Consoles.
Therefore, the Court finds Plaintiffs cannot plausibly allege that the misrepresentations
contained in these agreement induced them to purchase their Consoles. Accordingly, the
Court finds the Massachusetts, New Hampshire, and Texas negligent misrepresentations claims and the Michigan innocent misrepresentation claim each fail to allege a pecuniary loss.

Accordingly, the Court GRANTS Sony’s motion to dismiss the Florida, Massachusetts, Michigan, New Hampshire, and Texas negligent misrepresentations claims and the Michigan innocent misrepresentation claim. Because the Court’s prior order highlighted the deficiencies noted above, dismissal is without leave to amend. See Foman v. Davis, 371 U.S. 178, 182 (1962) (stating leave to amend need not be given when the party has been given prior opportunities to cure deficiencies).

C. Breach of Warranty Claims

Plaintiffs assert breach of warranty claims under Florida law (Count 7), Michigan law (Count 17), Missouri law (Count 24), New Hampshire law (Count 29), New York law (Count 34), Ohio law (Counts 40-41), and Texas law (Count 45). (FACC ¶¶ 222-227, 288-293, 334-339, 404-409, 371-376, 441-445, 467-472, 436-440.) Each claim essentially asserts the same factual basis for relief—Sony made affirmations of fact and/or promises to consumers regarding the adequacy and performance of Sony’s network security, and subsequently breached these promises by failing to provide adequate network security to protect Plaintiffs’ Personal Information.

Sony moves to dismiss each warranty claim on the basis that: (1) the choice-of-law provisions in the PSN and SOE User Agreements, upon which Plaintiffs base their claims, require any and all claims arising out of the agreements to be brought under California law; (2) Plaintiffs have failed to allege a cognizable injury; (3) Plaintiffs have failed to plead reliance; (4) Plaintiffs have failed to demonstrate that an express warranty has been breached; and (5) Plaintiffs cannot recover consequential, incidental, or special damages pursuant to limitation of damages clauses contained in the agreements. Because the Court finds the choice-of-law clauses in the PSN and SOE User Agreements require Plaintiffs to bring their breach of warranty claims under California law, which
Plaintiffs have not done, the Court does not addresses Sony’s remaining arguments for dismissal.  

1. Choice-of-Law Analysis

Sony contends each breach of warranty claim should be dismissed pursuant to the choice-of-law clauses in the PSN and SOE User Agreements because the agreements specify that any and all claims arising under the agreements must be brought under California law. (Doc. No. 94-2, Ex. A, SNE User Agreement; Doc. No. 135-2, Ex. 1, SOE User Agreement.) Sony further argues judicial estoppel supports this argument because Plaintiffs previously relied on the PSN and SOE User Agreements to support their UCL, FAL, and CLRA claims, and therefore can not now elect to contest the applicability of these agreements. (Doc. No. 78 ¶ 116; FACC ¶ 145). In response, Plaintiffs do not specifically address the applicability of the choice-of-law clauses, rather, Plaintiff argue that judicial estoppel does not bar their claims because they never asserted California breach of warranty claims, and they did not previously “achieve success” with regard to their UCL, FAL, and CLRA claims. The Court finds Plaintiffs’ judicial estoppel arguments fail to address the dispositive issue before the Court—the applicability and enforceability of the choice-of-law provisions.

In pertinent part, the PSN User Agreement states: “Except as otherwise required by applicable law, this Agreement shall be construed and interpreted in accordance with the laws of the State of California applying to contracts fully executed and performed within the State of California.” (Doc. No. 94-2, Ex. A at 9.) Similarly, the SOE User Agreement states: “This Agreement is governed in all respects by the substantive laws of the State of California and of the United States of America.” (Doc. No. 135-2, Ex. 1 at 32.) Therefore, based on the unambiguous language set forth above, the Court finds each of Plaintiffs’ breach of warranty claims is potentially subject to dismissal under the

25 Only Sony addressed the Court’s tentative ruling at oral argument, requesting that each warranty claim be dismissed without leave to amend.
choice-of-law clauses, subject only to the enforceability of the provisions under applicable law. See, e.g., *Wolph v. Acer Am. Corp.*, 272 F.R.D. 477, 485 (N.D. Cal. 2011).

To determine the enforceability of the choice-of-law clauses in the PSN and SOE User Agreements, the Court employs a two-step process. First, the Court must decide which forum’s choice-of-law rules apply; and second, the Court must decide whether the choice-of-law clauses are enforceable in each of the selected forum(s). Under the first determination, courts generally apply the choice-of-law rules of the forum in which the action is currently pending, which in this case would be California. See *Klaxon Co. v. Stentor Elec. Mfg.*, Co., 313 U.S. 487, 496 (1941). However, because the JPML transferred the instant litigation to this Court pursuant to 28 U.S.C. § 1407, the Court must apply the choice-of-law rules of each state where the individual actions were originally filed. (Doc. No. 1.) See, e.g., *In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prods. Liab. Litig.*, 785 F. Supp. 2d 925, 929 (C.D. Cal. 2011) (stating that although the cases in multidistrict litigation are before one court in one jurisdiction, they have been “effectively consolidated for pretrial purposes, the cases retain separate and distinct identities in preparation for their eventual return to their home states.”); *In re Nucorp Energy Sec. Litig.*, 772 F.2d 1486, 1492 (9th Cir. 1985).

Although this would normally be an arduous task, properly conducted by the parties rather than the Court, the Court finds further briefing on the issue unnecessary. Each of the cases filed by the eleven named Plaintiffs were originally filed in California.26


Accordingly, the Court employs California choice-of-law rules to determine the enforceability of the provisions.

a. Enforceability Under California Law

In deciding whether to enforce a contractual choice-of-law provision, California applies the Restatement (Second) Conflict of Laws Section 187, “which reflects a strong public policy favoring enforcement of such provisions.” *ABF Capital Corp. v. Osley*, 414 F.3d 1061, 1065 (9th Cir. 2005) (quoting *Hambrecht & Quist Venture Partners v. Am. Med. Int'l, Inc.*, 38 Cal. App. 4th 1532, 1544 (Cal. Ct. App. 1995)). Under Section 187, a court must first determine: “(1) whether [California] has a substantial relationship to the parties or the transaction, or (2) whether there is any other reasonable basis for the parties’ choice-of-law.” *ABF Capital Corp*, 414 F.3d at 1066; *see also Nedlloyd Lines B.V. v. Super. Ct.*, 3 Cal. 4th 459, 465 (Cal. 1992). If the court finds either condition has been met, California law will apply unless it is contrary to a fundamental policy of the state selected by the aggrieved party. *Nedlloyd*, 3 Cal. 4th at 466.

Here, although neither party analyzed whether the choice-of-law clauses in the PSN and SOE User Agreements are enforceable under Section 187, the allegations set forth in the FACC are sufficient to enable the Court to make this determination without further briefing. The FACC alleges that: (1) SCEA is a Delaware limited liability company with its principal place of business in Foster City, California, (FACC ¶ 30); (2) SNEA is a Delaware corporation that conducts business in California, (Id. at ¶ 31); (3) SNEI is a Delaware limited liability company with its principal place of business in Los Angeles, California, (Id. at ¶ 32); and (4) SOE is a Delaware limited liability company that has its principal place of business in Terman Court, San Diego, (Id. at ¶ 33). Therefore, because three of the four Sony Defendants (SCEA, SNEI, and SOE) have their principal place of business in California and the remaining Sony Defendant (SNEA) conducts business in the state of California, the Court finds California has a substantial relationship to the parties. *See, e.g., Ruiz v. Affinity Logistics Corp.*, 667 F.3d 1318, 1323 (9th Cir. 2012) (“A substantial relationship exists where one of the parties is
domiciled or incorporated in the chosen state.”); PAE Gov’t Servs., Inc. v. MPRI, Inc., 514 F.3d 856, 860 (9th Cir. 2007) (finding Virginia had a substantial relationship to one of the parties because the party had its principal place of business in Virginia).

Finding the first condition met, i.e., that California has a substantial relationship to the parties, the Court next determines whether California express warranty law is contrary to a fundamental policy of Florida, Michigan, Missouri, New York, New Hampshire, Ohio, or Texas express warranty law. The Court finds no conflict. In order to assert a claim for breach of warranty under California, Florida, Michigan, Missouri, New York, New Hampshire, Ohio, or Texas law a plaintiff must allege that: (1) the seller made a promise; (2) the buyer relied upon the seller’s promise; (3) the seller’s promise later turned out to be false; and (4) the plaintiff suffered injury as a result.27 Each state also requires a buyer to provide notice to the seller before bringing a breach of warranty claim.28

Therefore, based on the above, the Court finds the choice-of-law clauses in the PSN and SOE User Agreements enforceable and each of the warranty claims not alleged under California law should be dismissed. Moreover, because Plaintiffs did not bring


express warranty claims under California law, did not address Sony’s contentions that a
California breach of express warranty claim would nonetheless fail as a matter of law,
and explicitly alleged that California law should be applied to each of their claims
pursuant to the PSN and SOE User Agreements (FACC ¶ 145), the Court GRANTS
Sony’s motion to dismiss each of the express warranty claims without leave to amend.
See Civ. L.R. 7.1.f.3.b (“The opposition shall contain a brief and complete statement of
all reasons in opposition to the position taken by the movant, an answering memorandum
of all points and authorities, and copies of all documentary evidence which the party in
opposition relies.”); Missud v. Oakland Coliseum Joint Venture, No.12-02967 JCS, 2013
WL 3286193, at *11 (N.D. Cal. June 27, 2013) (dismissing claim without leave to amend
on the basis that further amendment would be futile in light of the opposing parties
failure to address the moving parties’ arguments).

D. Breach of Implied Warranty

Plaintiffs’ breach of implied warranty claims can be categorized into two sub-
groups—common law claims and statutory claims. Plaintiffs assert common law implied
warranty claims under Florida law (Count 8), Michigan law (Count 18), Missouri law
(Count 25), and New York law (Count 35), (FACC ¶¶ 228-233, 294-299, 340-345, 410-
415), and statutory implied warranty claims under Massachusetts law (Count 12), New
Hampshire law (Count 30), and Texas law (Count 46), (Id. at ¶¶ 250-255, 377-382, 473-
478). Each common law implied warranty claim alleges that Sony impliedly represented
and warranted that Sony Online Services provided adequate network security, when in
fact, Sony knew its network security was inadequate and vulnerable to intrusion. (Id. at
¶¶ 229-230, 295-296, 341-342, 411-412.) Similarly, each statutory implied warranty
claim alleges that by creating, marketing, and selling PS3s, PSPs, and Sony Online
Services, Sony impliedly represented and warranted that Sony Online Services and/or the
Network were merchantable, fit for their intended purposes, and provided adequate
security for Plaintiffs’ Personal Information. (Id. at ¶¶ 252, 378, 474.)
Sony moves to dismiss each implied warranty claim on the basis that: (1) Plaintiffs have not alleged a cognizable injury; (2) the common law claims fail because there is an express agreement between the parties governing the exact warranties at issue; (3) the statutory claims fail because network services are not “goods” as defined under the Uniform Commercial Code (“UCC”); and (4) the implied warranties were expressly disclaimed and/or expressly limited by clear and conspicuous language in the PSN User Agreement.29 (Doc. No. 135 at 26-30.) The Court finds Sony’s second, third, and fourth arguments fatal to Plaintiffs’ claims, and therefore does not address Sony’s remaining argument.30

1. Common Law Implied Warranties

First, Sony contends each common law implied warranty claim should be dismissed because implied terms are disfavored under common law where the parties have a written agreement that covers the exact terms at issue. Therefore, Sony argues the Florida, Michigan, Missouri, and New York implied warranty claims should be dismissed because they are based on the same factual allegations as Plaintiffs’ Florida, Michigan, Missouri, and New York express warranty claims. (Compare FACC ¶¶ 229, 295, 341, 411 with ¶¶ 223, 289, 335, 405.) Assuming without deciding that Plaintiffs would be permitted to pursue their implied warranty claims in the alternative to their breach of express warranty claims, as set forth below, the Court finds Plaintiffs’ common law implied warranty claims are subject to dismissal based on the disclaimer in the PSN User Agreement and the PSN Privacy Policy. (Doc. No. 94, Ex. A at 9, PSN User Agreement; Doc. No. 94, Ex. C at 4, PSN Privacy Policy.)

29 Sony argued in its reply brief that Plaintiffs’ implied warranty claims were also subject to dismissal based on the choice-of-law provision in the PSN User Agreement. However, because Sony’s motion to dismiss did not present this contention the argument is not properly before the Court. See United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006).

30 Neither party addressed the Court’s tentative ruling at oral argument, which stated that the implied warranty claims were subject to dismissal without leave to amend based on the disclaimer in the PSN User Agreement. (Doc. No. 157.)
2. Disclaimer of Implied Warranties

Second, as a general rule, statutory and common law implied warranties can be
disclaimed by conspicuous language in a contract presented to the consumer at the time
of the transaction.31 Here, before registering for the PSN, each Plaintiff was required to
consent to the PSN User Agreement and the PSN Privacy Policy. (FACC ¶¶ 40, 56, 57.)
In pertinent part, the PSN User Agreement contained the following disclaimer:

16. WARRANTY AND DISCLAIMER AND LIMITATION OF
LIABILITY

No warranty is given about the quality, functionality, availability or perfor-
mance of Sony Online Services or any content or service offered on or
though Sony Online Services. All services and content are provided “AS
IS” and “AS AVAILABLE” with all fault. SNEA does not warrant that the
service and content will be uninterrupted, error-free or without delays. In
addition to the limitations of liability in merchantability, warranty of fitness
for a particular purpose and warranty of non-infringement, SCEA assumes
no liability for any inability to purchase, access, download or use any
content, data, or service.

(Doc. No. 94, Ex. A at 9.) Although not labeled as a disclaimer, the PSN Privacy Policy
contained similar admonitory language regarding the adequacy of Sony’s network
security:

Accuracy & Security

We take reasonable measures to protect the confidentiality, security, and
integrity of the personal information collected from our website visitors . . .
Unfortunately, there is no such thing as perfect security. As a result,
although we strive to protect personally identifying information, we cannot
ensure or warrant the security of any information transmitted to us through
or in connection with our websites, that we store on our systems or that is
stored on our service providers’ systems.

31 See, e.g., Belle Plaza Condo. Ass’n, Inc. v. B.C.E. Dev., Inc., 543 So. 2d 239, 240
(Fla. Dist. Ct. App. 1989) (“Moreover, it is equally clear that B.C.E. properly disclaimed
by a bold and conspicuous disclaimer any and all express or implied warranties.”); Rokiesak v. Colony Marine Sales & Serv., Inc., 219 F. Supp. 2d 810, 815 (E.D. Mich.
2002) (stating that Michigan law allows for the disclaimer of implied warranties); Am.
(E.D. Mo. June 11, 2013) (same); Kraft v. Staten Island Boat Sales, Inc., 715 F. Supp. 2d
(“[Section 2-316] . . . seeks to protect a buyer from unexpected and un-bargained
language of disclaimer by denying effect to such language when inconsistent with
language of express warranty and permitting the exclusion of implied warranties only by
conspicuous language or other circumstances which protect the buyer from surprise.”);
Based on the above, both parties agree that Florida, Michigan, Missouri, New York, New Hampshire, and Texas law each allow a party to waive implied warranties, but waiver of implied warranties is prohibited under Massachusetts law.  

a. Florida, Michigan, Missouri, New York, New Hampshire, and Texas Implied Warranty Claims

Although the parties agree that Florida, Michigan, New York, New Hampshire, and Texas law permit the waiver of implied warranties, the parties disagree over whether the waiver was effective because it was made at the time Plaintiffs registered for the PSN and not at the time Plaintiffs purchased their Consoles. To the extent the waiver is ineffective, the parties also disagree over whether the limitation of damages provision is unconscionable. (Doc. No. 94, Ex. A at 9.)

After a review of the parties’ respective arguments, the Court finds the waiver effective. Plaintiffs’ contentions that the waiver was ineffective because it was made at the time Plaintiffs registered for the PSN and not at the time Plaintiffs purchased their Consoles is nonsensical, and representative of Plaintiffs’ continued attempts to bootstrap the purchase of a PSP or PS3 with registration for free PSN access. The FACC clearly alleges that Sony breached both common and statutory implied warranties by representing and warranting that Sony Online Services and/or the Network would provide adequate security for Plaintiffs’ Personal Information, when in fact, Sony knew its security was inadequate. (FACC ¶¶ 229, 295, 341, 378, 411, 474.) Thus, although Plaintiffs try to allege that the disclaimer in the PSN User Agreement and/or the PSN Privacy Policy was ineffective because it was not made at the time Plaintiffs purchased

32 Massachusetts is an exception to this general rule, enacting a provision that renders void any attempt to disclaim an implied warranty of merchantability or fitness for a particular purpose with regard to consumer goods. See Mass. Gen. Laws § 2-316A; Jacobs v. Yamaha Motor Corp., USA, 649 N.E.2d 758, 761 (Mass. 1995) (“Any language by which a manufacturer of consumer goods seeks to exclude or modify an implied warranty of merchantability or of fitness for a particular purpose, or to limit the consumer’s remedies for breach of those warranties, is unenforceable.”). Plaintiffs did not specifically address Sony’s contentions that the common law claims could be waived.
their Consoles, each implied warranty claim explicitly alleges that Sony Online Services and/or the Network—not Plaintiffs’ Consoles—failed to function as warranted. (Id.) This inconsistency in the FACC is further supported by the fact that Plaintiffs continue to rely on representations and warranties contained in the PSN User Agreement and the PSN Privacy Policy to support their claims, both of which were presented to Plaintiffs after they purchased their Consoles and before registering for free PSN access. Therefore, the Court finds the disclaimer effective because it was made at the time Plaintiffs bargained for free PSN access. *See Bowdoin v. Showell Growers, Inc.*, 817 F.2d 1543, 1545, 1546 n.11 (11th Cir. 1987) (observing that courts generally hold pre-sale disclaimers effective and collecting cases from state courts that conclude a post-sale disclaimer is not effective).

Finding the disclaimer applicable, the Court now examines the language of the disclaimer to determine the reach and effect of the disclaimer. As stated above, the PSN User Agreement states that “[a]ll services and content are provided ‘AS IS’ and ‘AS AVAILABLE’ with all faults.”33 (Doc. No. 94, Ex. A at 9.) The disclaimer also states that “any implied warranty of merchantability, warranty of fitness for a particular purpose[,] and warranty of non-infringement” was expressly disclaimed. (Id.) Similarly, the PSN Privacy Policy states that Sony does not “ensure or warrant the security of any information” transmitted to Sony over the network. (Doc. No. 94, Ex. C at 6.)

Therefore, based on the disclaimer and admonitory language in the PSN User Agreement and the PSN Privacy Policy, the Court finds the language clear and conspicuous. Read in conjunction, both documents explicitly disclaimed any and all claims arising under the implied warranty of merchantability, disclaimed any and all claims arising under the implied warranty of fitness for a particular purpose, stated in all caps that Sony Online Services would be provided “AS IS” and “AS AVAILABLE,” and informed consumers that Sony was not warranting the security of consumer personal

---

33 The Court does not consider the SOE User Agreement and SOE Privacy Policy because Plaintiffs did not bring an implied warranty claim under Ohio law.

**b. Massachusetts Implied Warranty Claim**

Finally, although the Massachusetts implied warranty claim cannot be disclaimed, the claim is nonetheless subject to dismissal under the UCC. See Mass. Gen. Law § 2-316A. Under Section 2 of the UCC, the implied warranty of merchantability and fitness for a particular purpose only applies to “transactions in goods.” Mass. Gen. Law § 2-102. The UCC defines “Goods” as “all things . . . which are movable at the time of identification to the contract for sale.” Mass. Gen. Law § 2-105(1). The rendition of services is not covered by Section 2. See *White v. Peabody Constr. Co.*, 434 N.E.2d 1015, 1021 (Mass. 1982). However, if a contract involves the sale of both goods and services, the court must consider whether the predominant factor, thrust, or purpose of the contract is: (1) “the rendition of [a] service, with goods incidentally involved (e.g., contract with artist for painting);” or (2) “is a transaction of sale, with labor incidentally involved (e.g., installation of a water heater in bathroom).” *Bonebrake v. Cox*, 499 F.2d 951, 960 (8th Cir. 1974).
Here, Plaintiffs allege that by “creating, marketing, and selling PS3s, PSPs, and Sony Online Services,” Sony “impliedly represented and warranted that the Network was merchantable, fit for its intended purposes, and provided adequate security.” (FACC ¶ 252.) Plaintiffs then define the “Network” as Sony’s computer systems, servers, and databases. (Id. at ¶ 4.) Therefore, based on Plaintiffs’ own allegations, Plaintiffs allege that the “Network,” i.e., Sony’s computer systems, servers, and/or databases were not merchantable or fit for their intended purposes—not Plaintiffs’ Consoles. Thus, because network services are not subject to the UCC because they are not physically “movable at the time of identification to the contract,” nor could PSN access be considered a good because it was offered free of charge, the Court finds Plaintiffs’ claim is barred by the UCC. Moreover, although Plaintiffs attempt to argue that this was a mixed transaction, because the purchase of a Console was a necessary prerequisite to obtain free PSN services, the Court is not persuaded. To the extent this was a mixed transaction, the trust or purpose of the contract was to provide free PSN access, with goods, i.e., the Console, incidentally involved. See, e.g., Bonebrake, 499 F.2d at 960; Ogden Martin Sys. of Indianapolis, Inc. v. Whiting Corp., 179 F.3d 523, 530 (7th Cir. 1999) (“As the party seeking the benefit of the UCC, Whiting bears the burden of establishing that the predominant thrust of the transaction was for goods and only incidentally for services.”).

Accordingly, based on the disclaimer in the PSN User Agreement, the admonitory language in the PSN Privacy Policy, and Plaintiffs’ failure to show that their Massachusetts statutory implied warranty claim falls within the purview of the UCC, the Court GRANTS Sony’s motion to dismiss the Florida, Michigan, Missouri, New York, New Hampshire, Texas, and Massachusetts implied warranty claims without leave to amend. See Pedigo v. Cnty. of L.A., 24 F. App’x 779, 785 (9th Cir. 2001) (“[A] district court does not abuse its discretion in denying leave to amend where the proposed amendment

34 As stated by Sony, and never once rebutted by Plaintiffs, the PSN is a free service and none of the Plaintiffs allege that they purchased premium PSN services.
would be futile or where the amended complaint would not withstand a motion to dismiss.

E. Unjust Enrichment Claims

Plaintiffs assert unjust enrichment claims under Florida law (Count 10), Massachusetts law (Count 13), Michigan law (Count 21), Missouri law (Count 23), New Hampshire law (Count 32), New York law (Count 36), Ohio law (Count 39), and Texas law (Count 48). (FACC ¶¶ 239-243, 256-261, 310-313, 329-333, 388-392, 416-420, 432-435, 484-488.) Each cause of action essentially alleges that Plaintiffs conferred benefits on Sony by purchasing, registering with, and/or sending their Personal Information to Sony Online Services, and that Sony was unjustly enriched in retaining revenues derived from these benefits. (Id. at ¶¶ 240-241, 257, 259, 311-312, 330-331, 389-390, 433-434, 485-486.) Sony moves to dismiss each claim on the basis that: (1) Plaintiffs cannot assert claims for unjust enrichment claims because an express contract governs the same subject matter at dispute between the parties; and (2) Plaintiffs have failed to allege a benefit conferred upon Sony that was wrongly retained.35

In response, Plaintiffs contend their unjust enrichment claims are properly plead in the alternative to their breach of contract claims. The Court, however, does not agree. Under Florida, Massachusetts, Michigan, Missouri, New Hampshire, New York, Ohio, and Texas law a plaintiff may not recover for unjust enrichment where a “valid, express contract governing the subject matter of the dispute exists.” Coghlan v. Wellcraft Marine Corp., 240 F.3d 449, 454 (5th Cir. 2001) (applying Texas law).36 Here, neither

35 Neither party addressed the Court’s tentative ruling at oral argument, which stated that each unjust enrichment claim was subject to dismissal without leave to amend based on the existence of a valid contract between the parties. (Doc. No. 157.)

party contests the validity of the PSN/SOE User Agreements and the PSN/SOE Privacy Policies, and Plaintiffs rely on these exact agreements to support their allegations. Therefore, because Plaintiffs do not argue that the agreements are somehow invalid or otherwise unenforceable, Plaintiffs are not permitted to plead unjust enrichment as an alternative to breach of contract claims. Accordingly, the Court GRANTS Sony’s motion to dismiss the Massachusetts, Texas, Florida, Missouri, New Hampshire, New York, Ohio, and Michigan law unjust enrichment claims without leave to amend. See Netbula, LLC v. Distinct Corp., 212 F.R.D. 534, 539 (N.D. Cal. 2003) (discussing futility of amendment when considering whether to grant leave to amend).

F. Consumer Protection Claims

Plaintiffs assert consumer protection claims under the California Unfair Competition Law (“UCL”) (Count 1), the California False Advertising Law (“FAL”) (Count 2), the California Consumer Legal Remedies Act (“CLRA”) (Count 3), the Florida Deceptive and Unfair Trade Practices Act (“FDUTPA”) (Count 6), the Michigan Consumer Protection Act (“MCPA”) (Count 16), the Missouri Merchandising Practices Act (“MMPA”) (Count 22), the New Hampshire Consumer Protection Act (“NHCPA”) (Count 28), the New York Deceptive Practices Act (“NYDPA”) (Count 33), the Ohio


An unjust enrichment claim may only be pled in the alternative to a breach of contract claim where one party asserts that the contract governing the dispute is invalid or the contract does not cover the subject matter at issue. See, e.g., In re Managed Care Litig., 185 F. Supp. 2d 1310, 1337-38 (S.D. Fla. 2002); Newman & Schwartz v. Asplundh Tree Expert Co., 102 F.3d 660, 663 (2d Cir. 1996) (allowing unjust enrichment claim to be pled in the alternative to a breach of contract claim under New York law because the defendant disputed whether plaintiff, a non-party to the contract, was an intended third-party beneficiary of the contract); Ajuba Int’l, LLC v. Saharia, 871 F. Supp. 2d 671, 692 (E.D. Mich. 2012) (allowing alternative pleading under Michigan law because it was unclear if any of the contracts covered the subject matter at issue and the defendants contested the validity of the contract); Miami Valley Mobile Health Servs., Inc. v. ExamOne Worldwide, Inc., 852 F. Supp. 2d 925, 939 (S.D. Ohio 2012) (allowing alternative pleading under Ohio law because the validity of the contract was not conceded by defendants and it was possible that the court could later find one or more of the contracts invalid); Manicini Enters., Inc. v. Am. Exp. Co., 236 F.R.D. 695, 699 (S.D. Fla. 2006) (allowing alternative pleading under Florida law because the existence of an express contract between the parties had not yet been established).
Consumer Sales Practices Act (“OCSPA”) (Count 37), the Ohio Deceptive Trade Practices Act (“ODTPA”) (Count 38), and the Texas Deceptive Trade Practices Act (“TDTPA”) (Count 44). On October 24, 2013, the Court ordered supplemental briefing on the FDUTPA, MCPA, MMPA, NHCPA, NYDPA, OCSPA, and the TDTPA causes of actions. (Doc. No. 159.) Because consumer protection claims are a “creature of the state in which they are fashioned,” the Court separately addresses the sufficiency of each claim. See Mazza v. Am. Honda Motor Co., 666 F.3d 581, 591 (9th Cir. 2012).

1. California Consumer Protection Claims

Plaintiffs’ first three causes of action allege Sony violated California’s consumer protection statutes—the UCL, the FAL, and the CLRA. (FACC ¶¶ 146-185.) Courts often analyze these statutes together because they share similar attributes. See, e.g., Paduano v. Am. Honda Motor Co., 169 Cal. App. 4th 1453, 1468–73 (Cal. Ct. App. 2009) (analyzing UCL and CLRA claims together); Anunziato v. eMachines, Inc., 402 F. Supp. 2d 1133, 1137 (C.D. Cal. 2005) (analyzing UCL and FAL together). The UCL prescribes business practices that are “unlawful, unfair or fraudulent,” Cal. Bus. & Prof. Code § 17200, the FAL prohibits the dissemination of any advertising “which is untrue or misleading,” Cal. Bus. & Prof. Code § 17500, and the CLRA declares specific acts and practices in the sale of goods or services to be unlawful, including making affirmative misrepresentations or omissions regarding the “standard, quality, or grade” of a particular good or service, Cal. Civ. Code § 1770(a). Under the UCL and FAL a plaintiff may only recover restitution and injunctive relief, whereas a plaintiff’s recovery under the CLRA is not so limited. See In re Vioxx Class Cases, 180 Cal. App. 4th 116, 130 (Cal. Ct. App. 2009) (UCL and FAL); Cal. Civ. Code § 1780(a)(1) (stating that the CLRA allows actual and punitive damages). Sony moves to dismiss the UCL, FAL, and CLRA claims on the basis that: (1) Plaintiffs do not have standing; (2) Plaintiffs have failed to plead unlawful, unfair, deceptive, or unconscionable conduct; (3) Plaintiffs have failed to plead any basis for restitution or injunctive relief under the UCL and FAL; and (4) the CLRA is inapplicable to the transactions at issue. Each is discussed in turn.
Standing Under the UCL, FAL, and CLRA

First, Sony contends Plaintiffs do not have standing under the UCL, FAL, or CLRA because the alleged misrepresentations and/or omissions did not result in a cognizable injury. As stated in the Court’s prior order, standing under the UCL and FAL is limited to individuals who can “(1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., economic injury, and (2) show that the economic injury was the result of, i.e., caused by, the unfair business practice or false advertising that is the gravamen of the claim.” Kwikset Corp. v. Super. Ct., 51 Cal. 4th 310, 322 (Cal. 2011) (holding that the UCL and FAL standing requirements are identical); Cal. Bus. & Prof. Code §§ 17204 (UCL), 17535 (materially identical standard under the FAL); Hinojos v. Kohl’s Corp., 718 F.3d 1098, 1104 (9th Cir. 2013). A plaintiff need not allege eligibility for restitution to establish standing under UCL and FAL. Id. at 335–36. Similarly, to establish standing under the CLRA, a plaintiff must allege that the defendant’s conduct resulted in a “tangible increased cost or burden to the consumer.” Meyer v. Sprint Spectrum LP, 200 P.3d 295, 301 (Cal. 2009). This requires showing “not only that a defendant’s conduct was deceptive[,] but that the deception caused them harm.” In re Vioxx Class Cases, 180 Cal. App. 4th at 129.

Here, Plaintiffs allege they lost money or property under the UCL and FAL because: (1) they lost the unencumbered use of their passwords; (2) their passwords were obtained by a third party without their consent; (3) they were unable to access Sony Online Services during the time the PSN was temporarily disabled; (4) certain applications and products that can only be accessed via the network were rendered worthless during the brief interruption in PSN service; and (5) their Consoles diminished in value as a result of Sony’s failure to secure the network and/or the extended time during which the network was disabled. (FACC ¶¶ 157-158, 168-169.) With respect to the CLRA, Plaintiffs allege that they were harmed as a result of Sony’s unlawful conduct because their Personal Information was compromised, they now have an increased risk of future identity theft, they lost the unencumbered use of their passwords, and their passwords...
were disclosed to third parties without their consent. Plaintiffs also allege that they lost money or property under the CLRA because their Consoles diminished in value as a result of: (1) Sony’s failure to secure their Personal Information; (2) the brief interruption in PSN services; and (3) the diminished value of products and services that could not be accessed during the brief interruption in PSN service. Although the Court does not readdress Plaintiffs’ previously dismissed contentions that their Personal Information has independent monetary value, (Doc. No. 120 at 21:11-16), under the unusual circumstances presented here, the Court finds Plaintiffs’ amended allegations have satisfied the standing requirement under the UCL, FAL, and CLRA based on Sony’s alleged omissions at the point of purchase of Plaintiffs’ Consoles.

As an initial matter, neither party disputes that the PSN was offered to Plaintiffs free of charge or that Plaintiffs registered for the PSN after acquiring their Consoles. Nonetheless, the parties ardently dispute whether Plaintiffs have sufficiently alleged a loss of money or property and/or harm that was “caused by” Sony’s alleged unfair business practices or deceptive conduct. Throughout the FACC, Plaintiffs contend that access to the PSN and the corresponding ability to access the Internet via their Consoles was a key feature of Plaintiffs’ Consoles, and that had Sony disclosed that the PSN was not reasonably secure and/or that Sony did not use industry-standard encryption to secure Plaintiffs’ Personal Information, Plaintiffs would not have purchased their Consoles and/or would not have paid as much for their Consoles.38 In response, Sony contends that Plaintiffs cannot plausibly allege that they relied on Sony’s alleged misrepresentations because each of the alleged representations were contained in the

38 The FACC alleges that Sony represented and/or omitted material information regarding the security of the PSN at the time Plaintiffs purchased or otherwise acquired their Consoles. (FACC ¶¶ 18-28, 29; Doc. No. 146 at 19-20.) Plaintiffs further allege that had they known that Sony did not utilize reasonable, adequate, or industry-standard security measures to protect Plaintiffs’ Personal Information transmitted to Sony before registering for the PSN, Plaintiffs, acting as reasonable consumers, would not have purchased their PS3s, would not have paid the same amount for their PS3s, and/or would not have provided their Personal Information to Sony. (FACC ¶ 29; Doc. No. 146 at 19:12-18.) Plaintiffs support these contentions by alleging that access to the PSN, although a free service, was a key feature of PS3s, and a major factor in Plaintiffs’ decision to purchase a PS3. (FACC ¶¶ 40, 41, 167.)
PSN User Agreement and/or the PSN Privacy Policy, both of which were presented to Plaintiffs after they purchased their Consoles. As a result, Sony argues the alleged misrepresentations and/or deceptive conduct could not have plausibly caused Plaintiffs harm.

Although the Court agrees with Sony, that Plaintiffs cannot plausibly rely on alleged misrepresentations contained within the PSN User Agreement and/or the PSN Privacy Policy, as these representations were presented to Plaintiffs after they purchased their Consoles, Sony’s arguments fail to address Plaintiffs’ fraudulent omission contentions. As set forth by the California Supreme Court in *Kwikset v. Superior Court*, 51 Cal. 4th 310, 323 (Cal. 2011), economic injury may result from unfair competition if a plaintiff: “(1) surrender[s] in a transaction more, or acquire[s] in a transaction less[] than he or she otherwise would have; (2) [has] a present or future property interest diminished; (3) [is] deprived of money or property to which he or she has a cognizable claim; or (4) [is] required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.” As a result, to the extent a consumer has “paid more for a product than he or she otherwise might have been willing to pay if the product had been labeled accurately,” the consumer has lost money or property regardless of whether the court “might objectively view the products as functionally equivalent.” *Id.* at 329. This reasoning holds true whether the plaintiff’s claim is based on affirmative misrepresentations or omissions. *See, e.g., Daugherty v. Am. Honda Motor Co., Inc.*, 144 Cal. App. 4th 824, 835 (Cal. Ct. App. 2006) (stating that omissions are actionable under the CLRA if the omission is “contrary to a representation actually made. . . [or] a fact the defendant was obliged to disclose”); *Tait v. BSH Home Appliances Corp.*, No. 10–00711, 2011 WL 3941387, at *2 (C.D. Cal. Aug. 31, 2011).

Therefore, although this is not a false advertising case, which was acknowledged by Plaintiffs at the October 18, 2013 motion hearing, *In re Tobacco II*, 46 Cal. 4th 298, 328 (Cal. 2009), is nonetheless instructive—a plaintiff alleging standing under the UCL, FAL, and CLRA need only allege that the defendant’s conduct, whether it be an affirmat-
tive misrepresentation or an actionable omission, was an “immediate” cause and not the “sole” cause of the plaintiff’s injury. As a result, because Plaintiffs have alleged that Sony omitted material information regarding the security of Sony Online Services, and that this information should have been disclosed to consumers at the time consumers purchased their Consoles, the Court finds Plaintiffs have sufficiently alleged a loss of money or property “as a result” of Sony’s alleged unfair business practices. See, e.g., Mirkin v. Wasserman, 5 Cal. 4th 1082, 1093 (Cal. 1993) (stating that omitted information is material if a plaintiff can allege that “had the omitted information been disclosed, one would have been aware of it and behaved differently”); Falk v. Gen. Motors Corp., 496 F. Supp. 2d 1088, 1095 (N.D. Cal. 2007) (stating that materiality is viewed from the prospective of the reasonable consumer); Donohue v. Apple, Inc., 871 F. Supp. 2d 913, 921 (N.D. Cal. 2012) (stating that the plaintiff satisfied the causation requirement by pleading that he would not have purchased the product and or would have asked for a timely refund had he known certain material facts). Accordingly, the Court DENIES Sony’s motion to dismiss the UCL, FAL, and CLRA claims based on Plaintiffs’ failure to allege standing.

b. Failure to Allege Unlawful, Unfair, or Deceptive Conduct

Second, even if Plaintiffs have standing to assert claims under the UCL, FAL, and CLRA, Sony contends each claim should be dismissed because Plaintiffs have failed to allege unlawful, unfair, or deceptive conduct in compliance with Rule 9(b). Under Rule 9(b), allegations sounding in fraud “must state with particularity the circumstances constituting fraud or mistake.” Fed. R. Civ. P. 9(b). Where claims allege a “unified course of fraudulent conduct and rely entirely on that course of conduct as the basis of that claim, . . . the claim is said to be ‘grounded in fraud’ or to ‘sound in fraud,’ and the pleading . . . as a whole must satisfy the particularity requirement of Rule 9(b).” Kearns, 567 F.3d at 1126 (applying Rule 9(b) standard to uphold dismissal of UCL and CLRA claims that Ford Motor Company and its “co-conspirator” dealerships knowingly misrepresented to the public that certain vehicles were “safer and more reliable”).
Here, Plaintiffs’ UCL, FAL, and CLRA claims each allege the same factual basis for relief. Plaintiffs contend that: (1) Sony failed to take reasonable precautions and/or use industry-standard encryption to protect Plaintiffs’ Personal Information, (FACC ¶¶ 149, 163, 178); (2) Sony was aware that its security systems were inadequate and failed to rectify these shortcomings, (Id. at ¶¶ 149, 163, 175); (3) Sony misrepresented that access to the PSN was a feature of PSPs and PS3s, (Id. at ¶¶ 151, 164, 180); (4) Sony misrepresented that online connectivity and the corresponding ability to connect to Sony Online Services and Third Party Services was a feature of PSPs and PS3s, (Id. at ¶¶ 152, 165, 180); (5) Sony’s omitted material information regarding the security of the PSN, (Id. at ¶¶ 155, 163, 175); and (6) Sony’s conduct was unlawful because it violated the FAL, CLRA, DBA, and Sony’s own Privacy Policies, (Id. at ¶ 153). Plaintiffs also allege that Sony’s acts, omissions, and misrepresentations induced Plaintiffs to purchase their Consoles, register for the PSN, provide their Personal Information to Sony, and purchase content from the Playstation Store. (Id. at ¶¶ 156, 166, 179). Accordingly, the Court finds each claim “sounds in fraud” and Plaintiffs must plead their misrepresentation and omission claims under the UCL, FAL, and CLRA with particularity under Rule 9(b). Kearns, 567 F.3d at 1126.

i. Fraud-Based Affirmative Misrepresentations

A plaintiff alleging fraudulent misrepresentations under the UCL, FAL, and CLRA must allege that he was exposed to the particular representation claimed to be deceptive. See, e.g., Baltazar v. Apple, Inc., No. CV-10-3231-JF, 2011 WL 588209, at *3–4 (N.D. Cal. Feb. 10, 2011); Minnick v. Clearwire US, LLC, 683 F. Supp. 2d 1179, 56 11md2258 AJB (MDD)

39 Plaintiffs allege Sony violated the following enumerated sections of the CLRA §§ 1770(a)(5), (7), (9), (14), and (16). (FACC ¶ 176.)

40 At the October 18, 2013 motion hearing, Plaintiffs contended that not all of their California consumer protection claims sounded in fraud. The Court does not agree. Each of Plaintiffs’ consumer protection claims alleges that Sony omitted or misrepresented material facts regarding the adequacy of its network security, and that Sony was aware that its network security was inadequate. Moreover, as stated in the Court’s prior order, Plaintiffs previously agreed with Sony that their consumer claims were subject to Rule 9(b)’s particularity requirements. (Doc. No. 120 at 25:8-13.)
1188 (W.D. Wash. 2010). This requires the plaintiff to identify the “‘the time, place, and content of the alleged fraudulent misrepresentation[]; the identity of the person engaged in the fraud; and the circumstances indicating falseness’ or ‘the manner in which [the] representations were false and misleading.’” *Genna v. Digital Link Corp.*, 25 F. Supp. 2d 1032, 1038 (N.D. Cal. 1997) (quoting *In re GlenFed Sec. Litig.*, 42 F.3d 1541, 1547–58 n.7 (9th Cir. 1994)). Under all three statutes, conduct is deemed deceptive or misleading if the conduct is likely to deceive a reasonable consumer. *See Williams v. Gerber Prods. Co.*, 552 F.3d 934, 938 (9th Cir. 2008). Although this determination is generally fact intensive, courts have granted motions to dismiss under the UCL, FAL, and CLRA on the basis that the alleged misrepresentations were not false, misleading, or deceptive as a matter of law. *See, e.g., Freeman v. Time, Inc.*, 68 F.3d 285, 290 (9th Cir. 1995) (stating that when the flyer was read as a whole, including the qualifying language, the plaintiff’s allegation that a particular statement was deceptive was dispelled); *Haskell v. Time. Inc.*, 857 F. Supp. 1392, 1398 (E.D. Cal. 1994) (stating that “statements, in context, are not misleading. It is clear from the exemplar that no reasonable addressee could believe that the mailing announced that the addressee was already the winner . . . .”).

Here, Plaintiffs allege that Sony: (1) misrepresented that access to the PSN was a feature of PSPs and PS3s; (2) misrepresented that online connectivity and the corresponding ability to access Sony Online Services and Third Party Services was a feature of PSPs and PS3s; (3) misrepresented the characteristics and quality of Sony’s network security; (4) misrepresented that Sony uses “reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from [its] website visitors;” and (5) misrepresented that Sony maintains security measures “to protect the loss, misuse, and alteration of” consumer Personal Information. (FACC ¶¶ 151-152, 164-165, 177, 180.) Sony contends each of Plaintiffs’ misrepresentation claims should be dismissed because Plaintiffs have failed to plead actionable misrepresentations and/or causation.
As stated in the Court’s prior order, Plaintiffs’ first two contentions are without merit. No reasonable consumer would believe that Sony’s representations regarding the network were meant to promise continued and uninterrupted access to Sony Online Services and/or that Sony was providing uninterrupted access to the PSN. (Doc. No. 120 at 26-27.) However, notwithstanding the Court’s prior order, Plaintiffs continue to advance these same misrepresentation contentions in the FACC. For example, the FACC points to two Internet links where Plaintiffs allege Sony misrepresented that PSN access and online connectivity were features of the PS3. However, neither of these links represent that Sony promised continuous and uninterrupted service, and the first link (regarding PSN access) directs consumers to the PSN User Agreement and the PSN Privacy Policy, both of which inform consumers that Sony “does not warrant that the service and content will be uninterrupted, error-free, or without delays.” (Doc. No. 94-2, Ex. A at 9.) Therefore, although Sony represented that access to the PSN and online connectivity were features of Sony Consoles, Sony also informed consumers that continuous PSN access and/or Internet connectivity was not guaranteed without interruption. Accordingly, similar to Freeman v. Time, wherein the Ninth Circuit held that the defendant’s alleged misrepresentations were not misleading as a matter of law, here the PSN User Agreement clearly stated that access to the PSN and online connectivity may be interrupted. 68 F.3d at 290.

However, the Court finds Plaintiffs’ final two contentions are sufficiently plead. Plaintiffs allege that Sony misrepresented that it would take “reasonable steps” to secure Plaintiffs’ Personal Information, and that Sony Online Services used industry-standard encryption to prevent unauthorized access to sensitive financial information.” (Doc. No. 94-2, Ex. B at 6.) Although Sony seeks to combat these allegations by stating that Sony disclaimed any right to so-called “perfect security,” the Court agrees with Plaintiffs that whether or not Sony’s representations regarding “reasonable security” were deceptive, in

light of Sony’s additional representations regarding “industry-standard” encryption, are questions of fact not suitable for disposition on a motion to dismiss. Thus, because Sony made competing, potentially ambiguous representations, the Court cannot find the representations were not deceptive as a matter of law. See Lavie v. Procter & Gamble Co., 105 Cal. App. 4th 496, 508 (Cal. Ct. App. 2003) (“A perfectly true statement couched in such a manner that it is likely to mislead or deceive the consumer, such as by failure to disclose other relevant information,” is actionable). This determination is more properly adjudicated after discovery regarding Sony’s use or non-use of industry-standard encryption. Accordingly, the Court GRANTS Sony’s motion to dismiss the UCL, FAL, and CLRA claims based on affirmative misrepresentations regarding Plaintiffs’ ability to access the PSN and connect to the Internet, and DENIES Sony’s motion to dismiss Plaintiffs’ claims based on affirmative misrepresentations contained within the PSN User Agreement and the PSN Privacy Policy regarding “reasonable security” and “industry-standard encryption.” (FACC ¶¶ 149-150, 155, 163, 175.)

i. Fraud-Based Omissions

In addition to affirmative misrepresentations, the FACC now alleges fraud-based omission claims under the UCL, FAL, and CLRA. To be actionable under all three California consumer protections statutes, an omission must be “contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose.” Daugherty, 144 Cal. App. 4th at 835. A duty to disclose may arise: (1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; or (4) when the defendant makes partial representations but also suppresses some material fact. Falk, 496 F. Supp. 2d at 1094–95 (citing LiMandri v. Judkins, 52 Cal. App. 4th 326, 337 (Cal. Ct. App. 1997)).

Here, Plaintiffs allege that Sony: (1) failed to tell consumers that it did not have reasonable and adequate safeguards in place to protect consumers’ confidential informa-
tion; (2) failed to immediately notify members of the California subclass that the intrusion had occurred; and (3) omitted material facts regarding the security of its network, including the fact that Sony failed to install and maintain firewalls and utilize industry-standard encryption. Sony does not separately address Plaintiffs’ fraud-based omission claims. Rather, Sony contends Plaintiffs’ omission claims fail because Sony clearly disclosed the possibility of an intrusion. However, as discussed above with respect to statutory standing under the UCL, FAL, CLRA, the Court finds Plaintiffs’ fraud-based omission claims are sufficiently plead. Accordingly, the Court DENIES Sony’s motion to dismiss Plaintiffs’ claims under the UCL, FAL, and CLRA based on fraudulent omissions.

c. Restitution and Injunctive Relief Under the UCL and FAL

Third, Sony contends the UCL and FAL claims should be dismissed because Plaintiffs have failed to allege any basis for restitution and/or injunctive relief—the only two remedies allowed under the UCL and FAL. Although the Court previously dismissed Plaintiffs’ restitution claims with prejudice, Plaintiffs’ amended allegations have persuaded the Court to reconsider its prior ruling. (Doc. No. 120 at 29:4-30:3.) As set forth above, the FACC now clarifies that Plaintiffs seek restitution based on the fact that Sony benefitted financially from the sale of PSPs and PS3s, which was made possible and enhanced by Sony’s fraudulent omissions. (Doc. 146 at 27:7-8.) Therefore, to the extent Plaintiffs’ can prevail on their fraud-based omission claims, the Court finds Plaintiffs may be able to recover the purchase price of their Consoles or a portion thereof. Accordingly, the Court DENIES Sony’s motion to dismiss Plaintiffs’ claims for restitution under the UCL and FAL.

However, with regard to Plaintiffs’ claims for injunctive relief under the UCL and FAL, the Court previously dismissed theses claims for failure to allege the specific relief sought. (Doc. No. 120 at 29:25-30:3.) Plaintiffs’ acknowledged this deficiency at the September 27, 2012 motion hearing, stating that amendment would allow Plaintiffs to correct the pleading error. Plaintiffs have failed to do so. Accordingly, the Court
GRANTS Sony’s motion to dismiss Plaintiffs’ claims for injunctive relief without leave to amend. See Sisseton-Wahpeton Sioux Tribe of Lake Traverse Indian Res., N.D. & S.D. v. United States, 90 F.3d 351, 355–56 (9th Cir. 1996) (stating that a district court does not abuse its discretion to dismiss a complaint without leave to amend if a plaintiff was previously given an opportunity to correct noted deficiencies).

d. Applicability of the CLRA

Finally, Sony contends Plaintiffs’ CLRA claim should be dismissed because it is inapplicable to the transactions at issue—registration for free PSN services. The Court previously dismissed the CLRA claim with leave to amend on these exact grounds, finding that the claim was specifically linked to Plaintiffs’ registration for the PSN, which is neither a good nor a service under the CLRA. However, as acknowledged above, the FACC now alleges liability under the CLRA based on omissions that occurred at the point of purchase of Plaintiffs’ Consoles. (FACC ¶ 176.) Daugherty, 144 Cal. App. 4th at 835 (stating that a “claim may be stated under the CLRA in terms constituting fraudulent omissions”); Herron v. Best Buy Co., 924 F. Supp. 2d 1161, 1175 (E.D. Cal. 2013) (stating that fraudulent omission claims apply equally to claims under the CLRA). Therefore, although the Court still finds Plaintiffs’ CLRA claim cannot proceed based on affirmative misrepresentations, because those relate solely to the PSN, the CLRA claim may proceed on the basis that Sony omitted material information regarding the security of the PSN at the time Plaintiffs purchased their Consoles. Accordingly, the Court DENIES Sony’s motion to dismiss the CLRA claim.

2. Florida Deceptive and Unfair Trade Practices Act

Count 6 is brought by Plaintiffs Lieberman and Schucher and alleges violation of the FDUTPA. (FACC ¶¶ 212-221.) The FDUTPA prohibits “[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Fla. Stat. § 501.204(1); see also Delgado v. J.W. Courtesy Pontiac GMC-Truck, Inc., 693 So. 2d 602, 605-06 (Fla. 1997) (discussing the purpose of the FDUTPA in light of its legislative history). Plaintiffs allege Sony
violated the FDUTPA by falsely representing the security of Sony Online Services and request injunctive relief, declaratory relief, actual damages, and attorneys’ fees and costs. See Fla. Stat. § 501.211(1) (injunctive and declaratory relief), § 501.211(2) (actual damages and attorney’s fees and court costs), § 501.2105 (attorney’s fees). Sony moves to dismiss the FDUTPA claim on the basis that Plaintiffs have failed to allege: (1) actual loss caused by Sony’s conduct; and (2) unfair or deceptive acts or practices entitling Plaintiffs to declaratory or injunctive relief. (Doc. No. 163 at 1-6.)

a. Actual Damages Caused by Sony’s Deceptive and Unfair Conduct

As an initial matter, Sony contends the FDUTPA claim should be dismissed because Plaintiffs have not alleged actual damages caused by Sony’s deceptive or unfair conduct. The Court agrees. To state a claim under the FDUTPA, a consumer must allege: “(1) a deceptive act or unfair practice; (2) causation; and (3) actual damages.” Rollins, Inc. v. Butland, 951 So. 2d 860, 869 (Fla. Dist. Ct. App. 2006), review denied, 962 So.2d 335 (Fla. 2007); see also Virgilio v. Ryland Grp., Inc., 680 F.3d 1329, 1338 n.25 (11th Cir. 2012). Florida courts have defined “actual damages” as the “difference in the market value of the product or service in the condition in which it was delivered and its market value in the condition in which it should have been delivered according to the contract of the parties.” Rollins, Inc. v. Heller, 454 So. 2d 580, 585 (Fla. Dist. Ct. App. 1984) (internal citations omitted); Butland, 951 So. 2d at 869. “Nominal damages, speculative losses, or compensation for subjective feelings of disappointment” are not recoverable under the FDUTPA, Butland, 951 So. 2d at 873, nor may a Plaintiff recover “consequential damages,” Urling v. Helms Exterminators, Inc., 468 So. 2d 451, 454 (Fla. Dist. Ct. App. 1985).

---

42 Section 501.211(a) states: “In any action brought by a person who has suffered a loss as a result of a violation of this part, such person may recover actual damages, plus attorney’s fees and court costs as provided in s. 501.2105. However, damages, fees, or costs are not recoverable under this section against a retailer who has, in good faith, engaged in the dissemination of claims of a manufacturer or wholesaler without actual knowledge that it violated this part.”
Here, Plaintiffs Lieberman and Schucher seek to recover: (1) the purchase price of their Consoles and/or the amount they overpaid for their Consoles; (2) monthly premiums paid for Third Party Services during the time Plaintiffs were unable to access these services via their Consoles; and (3) the value of their Personal Information that was wrongfully disclosed. As explained below, none of these injuries are “actual damages” recoverable under the FDUTPA. *Fitzpatrick v. Gen. Mills, Inc.*, 263 F.R.D. 687, 695 (S.D. Fla. 2010), vacated on other grounds, 635 F.3d 1279 (11th Cir. 2011) (stating that although “subjective evidence of reliance” is not required, a plaintiff still must allege that “an objective reasonable person would have behaved” differently but for the alleged deceptive or unfair conduct).

First, although Plaintiffs’ supplemental brief contends that Plaintiffs suffered actual damages in the form of the purchase price of their Consoles, because they bargained for secure access to the PSN at the time they purchased their Consoles, the FACC does not support these contentions. (Doc. No. 164 at 5-7.) Rather, the FACC merely alleges that Plaintiffs were aggrieved by Sony’s deceptive and unfair conduct “in that they registered with, and sent their Personal Information to Sony Online Services after exposure to Defendants’ false and misleading representations regarding the security of Sony Online Services.” (FACC ¶ 218.) Nowhere does the FDUTPA claim allege that Plaintiffs would not have purchased their Consoles but for Sony’s alleged deceptive or unfair conduct. *See, e.g.*, *Pa. ex rel. Zimmerman v. PepsiCo, Inc.*, 836 F.2d 173, 181 (3d Cir. 1988) (“[I]t is axiomatic that the complaint may not be amended by the briefs in opposition to a motion to dismiss.”).

Moreover, even if the Court were to entertain Plaintiffs’ unpled contentions, which it will not, Plaintiffs have failed to allege that an “objective reasonable person would have behaved” differently absent the alleged deceptive or unfair conduct. *Fitzpatrick*, 263 F.R.D. at 695. For example, although Plaintiffs allege that Sony misled consumers as to the security of Sony Online Services, and that this deceptive conduct induced consumers to purchase their Consoles, or to purchase Consoles at an inflated price,
Plaintiffs concede that the alleged misrepresentations were contained in the PSN User Agreement and/or the PSN Privacy Policy—both of which were presented to consumers after they purchased their Consoles. As a result, Plaintiffs have failed to plausibly allege that the purchase price of their Console was an “actual damage” caused by Sony’s deceptive or unfair conduct. *Cf. Smith v. Wm. Wrigley Jr. Co.*, 663 F. Supp. 2d 1336, 1339–40 (S.D. Fla. 2009) (allowing plaintiff to recover on a benefit of the bargain theory because the plaintiff alleged that they relied on the defendant’s representations, and as a result of the alleged misleading representations, the defendant was able to charge a price premium for the product).

Second, Plaintiffs allege that they suffered actual injury because they paid monthly premiums for Third Party Services and were unable to access these services during the brief interruption in PSN access. However, similar to the reasons sets forth above, these allegations fail to set forth a plausible claim for relief. Plaintiffs did not advance these damage theories in the FACC (with respect to the FDUTPA claim), nor would such allegations suffice had they been properly pled. For example, as stated by the court in *Urling v. Helms Exterminators, Inc.*, 468 So. 2d 451, 454 (Fla. Dist. Ct. App. 1985), which considered on appeal whether the plaintiff had been awarded the proper measure of damages against a termite inspection company who issued a favorable report when no inspection had in fact been made, consequential damages are not permitted under the FDUTPA. Therefore, just as the plaintiff in *Urling* could not recover the cost of repairing extensive termite damage following the issuance of a fabricated termite report, here Plaintiffs are not permitted to recover monthly premiums paid to Third Party Services. *See, e.g.*, *Orkin Exterminating Co. v. Petsch*, 872 So. 2d 259, 263 (Fla. Dist. Ct. App. 2004) (stating that the FDUTPA only permits a consumer to recover the “diminished value” of the good or service received, consequential damages are not recoverable); *Kia Motors Am. Corp. v. Butler*, 985 So. 2d 1133, 1140 (Fla. Dist. Ct. App. 2008) (finding that recovery of repair and replacement costs are not recoverable under the FDUPTA); Fla. Stat. § 501.212(3); *In re Crown Auto Dealerships, Inc.*, 187 B.R.
1009, 1018 (Bankr. M.D. Fla. 1995) (holding claimants entitled to no recovery where they failed to establish that they suffered actual damages as a result of the misrepresentations about the vehicles; claimants subjective feelings of disappointment are insufficient to form a basis of actual damages). The same could be said for any recovery based on the brief interruption in PSN access, as the PSN was provided free of charge and Sony clearly disclaimed any right to uninterrupted access. (Doc. No. 94-2, Ex. A at 9.)

Finally, although Plaintiffs’ third contention is supported by the FACC, in that the FACC alleges that Plaintiffs would not have sent their Personal Information to Sony had they known the truth regarding Sony’s network security, these allegations fail to allege “actual damages” under the FDUTPA. As stated by the court in *Burrows v. Purchasing Power, LLC*, No. 1:12-cv-22800-UU, 2012 WL 9391827, at *3 (S.D. Fla. Oct. 18, 2012), which considered whether the disclosure of the plaintiff’s personal information without his consent gave rise to a claim under the FDUTPA, “[p]ersonal data does not have an apparent monetary value that fluctuates like the price of goods or services.” As a result, to the extent Plaintiffs are alleging an entitlement “to the value of their Personal Information,” but have not alleged a monetary loss relating to the disclosure of their Personal Information, these allegations fail under Florida law. *See Himes v. Brown & Co. Secs. Corp.*, 518 So. 2d 937, 938 (Fla. Dist. Ct. App. 1987) (finding no recovery under FDUTPA for misleading and false advertisement where plaintiff sustained no out-of-pocket losses); *Macias v. HBC of Fla., Inc.*, 694 So. 2d 88, 90 (Fla. Dist. Ct. App. 1997) (stating that to be entitled to any relief under FDUTPA the consumer must plead and prove he was aggrieved by the unfair and deceptive act).

Therefore, the Court finds Plaintiffs have failed to allege “actual damages” flowing from Sony’s alleged deceptive or unfair misrepresentations, nor would further amendment correct these deficiencies. Accordingly, the Court GRANTS Sony’s motion to dismiss the FDUTPA claim seeking actual damages without leave to amend. *See, e.g.*, *Sisseton-Wahpeton Sioux Tribe*, 90 F.3d at 356 (stating that the district court did not err in denying leave to amend because the plaintiff acknowledged that the claim was similar
to claims previously asserted); *Int'l Star Registry of Ill. v. Omnipoint Mktg., LLC*, 510 F. Supp. 2d 1015, 1024 (S.D. Fla. 2007).

b. Deceptive or Unfair Conduct Warranting Declaratory and Injunctive Relief Under the FDUTPA

Next, Sony moves to dismiss the declaratory and injunctive relief claims on the basis that Plaintiffs have failed to allege deceptive or unfair conduct under the FDUTPA. Specifically, Sony contends Plaintiffs have failed to: (1) allege deceptive or unfair conduct with particularity under Rule 9(b); (2) plausibly allege how Sony’s representations were deceptive in light of the admonitory language in the PSN Privacy Policy; (3) show how Sony violated Fla. Stat. § 500.04 and 21 U.S.C. § 343 because both statutes pertain to misbranded food; and (4) allege how Sony’s conduct was unfair in light of the fact that Plaintiffs have not alleged a single instance of identity theft or unreimbursed charges. The Court only addresses Sony’s second and fourth contentions.43

Under the FDUTPA, a deceptive practice is one that is “likely to mislead” consumers, *Davis v. Powertel, Inc.*, 776 So. 2d 971, 974 (Fla. Dist. Ct. App. 2000), and an unfair practice is one that “offends established public policy” or is “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers,” *Samuels v. King Motor Co. of Fort Lauderdale*, 782 So. 2d 489, 499 (Fla. Dist. Ct. App. 2001) (quoting *Spiegel, Inc. v. Fed. Trade Comm'n*, 540 F.2d 287, 293 (7th Cir. 1976)). A plaintiff need not allege an entitlement to “actual damages” in order to seek injunctive and/or declaratory relief under the FDUTPA, and must only allege a violation of the statute. See, e.g., Fla. Stat. § 501.211(1) (“[A]nyone aggrieved by a violation of this part may bring an action to obtain a declaratory judgment that an act or practice violates this part and to enjoin a person who has violated, is violating, or is otherwise likely to violate this part.”); *Wyndham Vacation Resorts, Inc. v. Timeshares Direct, Inc.*, 123 So. 3d 1149, 1152 (Fla. Dist. Ct. App. 2012).

43 Plaintiffs did not address Sony’s third contention and it appears these statutes were erroneously included in the FACC.
Therefore, although Sony contends that the representations in the PSN User Agreement and the PSN Privacy Policy could not have plausibly been deceptive or unfair in light of admonitory language in the PSN Privacy Policy, which disclaimed any right to so-called “perfect security,” Plaintiffs have refashioned their allegations to escape dismissal. As exemplified in the FACC and Plaintiffs’ opposition, Plaintiffs do not allege that Sony’s representations were deceptive because Sony promised perfect security (which was clearly disclaimed), Plaintiffs allege Sony violated the FDUTPA because Sony warranted that it would take “reasonable security” measures, including utilizing “industry-standard encryption”, but failed to do so. (FACC ¶¶ 3, 57, 62, 88, 97.) Thus, as discussed above, Plaintiffs have raised an issue of fact as to whether Sony’s representations, when viewed as a whole, were deceptive.44 See Siever v. BWGaskets, Inc., 669 F. Supp. 2d 1286, 1293 (M.D. Fla. 2009) (“Whether particular conduct constitutes such an unfair or deceptive trade practice is a question of fact.”).45 Accordingly, because declaratory and injunctive relief under the FDUTPA are available in the absence of actual damages, the Court DENIES Sony’s motion to dismiss Plaintiffs’ injunctive and declaratory relief claims under the FDUTPA.

3. Michigan Consumer Protection Act

Count 16 is brought by Plaintiff Mitchell and alleges violation of the MCPA. (FACC ¶¶ 276-287.) The MCPA prohibits “[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce[.]” Mich. Comp. Laws Ann. § 445.903(1). A plaintiff can pursue a claim under the MCPA based on fraud, deception, or breach of express or implied warranties. See Parsley v. Monaco Coach Corp., 327 F. Supp. 2d 797, 807 (W.D. Mich. 2004). Here, Plaintiffs allege Sony

44 This is true even though the PSN Privacy Policy states that “we cannot ensure or warrant the security of any information transmitted to us through [the PSN] . . . .” (Doc. No. 94-2, Ex. B at 6.)

45 The Court also finds Sony’s contentions regarding the interpretations of the FTC unavailing. The FACC properly alleges numerous and systematic vulnerabilities that Sony was allegedly aware of before the intrusion. Therefore, taking Plaintiffs’ allegations as true, which the Court must on a motion to dismiss, Plaintiffs have sufficiently alleged deceptive or unfair conduct under the FDUTPA.
violated the MCPA by “misleading the consuming public into believing that their
Personal Information would be safe upon transmission to Defendants[,] when in fact[,] Defendants knew that their security systems were woefully inadequate.” (FACC ¶ 281.)

Although not labeled as such in the FACC, Plaintiffs contend this conduct is grounded in both fraud and breach of express and implied warranties. Plaintiffs allege Sony violated the following sections of the MCPA:

(c) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that he or she does not have . . .

(e) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another . . .

(bb) Making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is . . .[and]

(cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

Mich. Comp. Laws § 445.903(1)(c), (e), (bb), (cc). Sony moves to dismiss the MCPA claim on the basis that Plaintiffs have failed to allege: (1) actual damages caused by a violation of the statute; and (2) a violation of the statute warranting declaratory or injunctive relief.

a. Actual Damages Under the MCPA

Plaintiffs seek the following actual damages under the MCPA: (1) the disclosure of their Personal Information and a corresponding loss in privacy; (2) the purchase price of their Consoles or a portion thereof; and (3) the inability to access Sony Online Services during the brief interruption in PSN access. (FACC ¶ 282.) Sony contends none of these damage allegations suffice because: (1) Plaintiffs have failed to plead reliance on the alleged misrepresentations in compliance with Rule 9(b); and (2) Sony Online Services was offered free of charge and Sony clearly disclaimed any right to uninterrupted access. Plaintiffs do not dispute that the potential risk of future identity theft resulting from the loss of personal information is not a cognizable injury under
Michigan law. Hammond v. The Bank of N.Y. Mellon Corp., No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *1, 8 (S.D.N.Y. June 25, 2010); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 782 (W.D. Mich. 2006). Therefore, the Court only addresses whether Plaintiffs have sufficiently pled reliance on Sony’s alleged misrepresentations, thereby entitling Plaintiffs to recover the purchase price of their Consoles and/or any damage relating to the inability to access Sony Online Services during the brief interruption in PSN access.

As an initial matter, the parties dispute whether Plaintiffs are required to plead actual reliance on the alleged misrepresentations, and to the extent actual reliance is required, whether reliance must be pled with particularity under Rule 9(b). Sony contends that pursuant to Mich. Comp. Laws Ann. Section 445.911(3), and countless Michigan courts interpreting the MCPA, Plaintiffs must allege actual reliance on Sony’s alleged deceptive conduct with specificity under Rule 9(b). In response, Plaintiffs argue that actual reliance is not required, and to the extent reliance is required, Plaintiffs have sufficiently alleged that Mitchell relied on Sony’s alleged misrepresentations. The Court agrees with Sony on both points.

First, although Plaintiffs attempt to rely on Dix v. American Bankers Life Assurance Co. of Florida, 415 N.W.2d 206, 209 (Mich. 1987), and Gasperoni v. Metabolife, International Inc., No. 00-71255, 2000 WL 33365948 (E.D. Mich. Sept. 27, 2000), for the proposition that reliance can be demonstrated by pleading that a “reasonable person would have relied on the representation,” both Dix and Gasperoni fail to address the pertinent issue before the Court—whether a named plaintiff in a putative class action must allege actual reliance. As a result, the Court finds Dix and Gasperoni fail to support Plaintiffs’ contentions, and cases discussing Dix and Gasperoni confirm that although class allegations can be based on what a reasonable person would have relied upon, a named plaintiff bringing a putative class action under the MCPA must still allege actual reliance. See, e.g., Kussy v. Home Depot USA Inc., No. 06-12899, 2006 WL 3447146, at *5–7 (E.D. Mich. Nov. 28, 2006); In re OnStar Contract Litig., 278 F.R.D. 69
352, 378 (E.D. Mich. 2011) (stating that there is “no dispute” that individuals asserting MCPA claims “must establish reliance”); Williams v. Scottrade, Inc., No. 06–10677, 2006 WL 2077588, at *7 (E.D. Mich. July 24, 2006) (dismissing a plaintiff’s MCPA claim premised on allegations of fraud because the plaintiff failed to identify the specific statements on which he relied); Mayhall v. A.H. Pond Co., 341 N.W.2d 268, 270 (Mich. 1983) (stating that the MCPA requires a plaintiff “to have sustained a loss as a condition for bringing an action to recover damages [because] . . . the Legislature . . . has incorporated . . . the common-law requirement of injury”). Accordingly, the Court finds Plaintiffs must allege that Mitchell actually relied on Sony’s alleged misrepresentations.

Second, although Plaintiffs are correct, that Rule 9(b) is inapplicable to MCPA claims based on breach of warranty rather than fraud, as stated above, the Court dismissed Plaintiffs’ breach of express and implied warranty claims under Michigan law. See Michels v. Monaco Coach Corp., 298 F. Supp. 2d 642, 651 (E.D. Mich. 2003); Sautner v. Fleetwood Enters., Inc., No. 05-73252, 2007 WL 1343806, at *6 (E.D. Mich. May 8, 2007) (“If there is no basis for a breach of warranty claim, it follows, then, that there is no basis for a MCPA claim based on the alleged breach.”). Therefore, the Court finds Plaintiffs’ allegations must be plead with particularity under Rule 9(b).

Based on the above, the Court finds Plaintiffs have failed to sufficiently allege that Mitchell actually relied on Sony’s alleged deceptive conduct in compliance with Rule 9(b). With regard to Plaintiffs’ allegations that they paid for their Consoles “after being exposed” to Sony’s alleged misrepresentations, this argument has already been disposed of by the Court. Each of the alleged misrepresentations identified by Plaintiffs are either contained in the PSN User Agreement and/or the PSN Privacy Policy, both of which were presented to Plaintiffs after they purchased their Consoles and before registering for the PSN. This is only further supported by the fact that Plaintiffs have conceded that they purchased their Consoles before reviewing the language in either agreement. Accordingly, even though the Court must accept Plaintiffs’ allegations as true, including the fact that Mitchell “relied” on Sony’s alleged misrepresentations in purchasing her
Console, Plaintiffs’ other allegations clearly contradict these conclusory allegations of reliance. See Regan v. Washtenaw Cnty. Rd. Comm’rs, 667 N.W.2d 57, 65 (Mich. 2003) ("We accept as true the allegations in the plaintiff’s complaint to the extent that affidavits or other documents submitted by the movant do not specifically contradict them."). As a result, Plaintiffs can not recover the purchase price of their Consoles, or a portion thereof, as actual damages under the MCPA.

The Court also finds Plaintiffs have failed to state a claim for actual damages relating to the brief interruption in Sony Online Services. As advanced by Sony and previously recognized by the Court, Sony Online Services were provided to Plaintiffs free of charge, Plaintiff Mitchell did not pay for premium services, and Sony clearly disclaimed any right to continuous and uninterrupted service. Thus, even though Plaintiffs correctly point out that a “frustration of a plaintiff’s expectations” can constitute a “loss” under the MCPA, Mitchell’s expectation of uninterrupted service was not reasonable, nor could Mitchell have had an “expectation” of uninterrupted service. Mayhall, 341 N.W.2d at 272; (Doc. No. 94-2, Ex. A at 9) (“SNEA does not warrant that the service and content will be uninterrupted, error-free or without delays.”). As a result, Plaintiffs can not recover actual damages resulting from a brief interruption in Sony Online Services under the MCPA. Accordingly, the Court finds Plaintiffs have failed to sufficiently allege a legal entitlement to actual damages under the MCPA based on either the purchase of their Consoles or the brief interruption in Sony Online Services. Because further amendment of this claim would be futile, the Court GRANTS Sony’s motion to dismiss the MCPA claim seeking actual damages without leave to amend.

b. Declaratory and Injunctive Relief

Sony also moves to dismiss Plaintiffs’ claims for injunctive and declaratory relief on the basis that Plaintiffs have neither alleged a violation of the MCPA, nor have Plaintiffs alleged why such relief is necessary. The Court does not agree. First, under the MCPA a plaintiff can seek declaratory and/or injunctive relief in the absence of actual damages. Therefore, taking the allegations set forth in the FACC as true, to the
extent Plaintiffs have alleged that Sony misrepresented the security of its network, including the fact that it utilized industry-standard encryption to secure Plaintiffs’ Personal Information, Plaintiffs have set forth a viable claim under Sections 445.903(1)(c), (e), (bb), and (cc). Moreover, Sony’s reliance on *Workmon v. Publishers Clearing House*, 118 F.3d 457, 458 (6th Cir. 1997), is misplaced. In *Workmon*, the Sixth Circuit affirmed the district court’s dismissal of the MCPA claim on the basis that no reasonable consumer would believe that they won a ten million dollar sweepstakes in light of admonitory language included in the flyer. *Id.* at 458–59 (stating that the “MCPA and Michigan case law provide no remedy for a trade practice that is confusing only to an unreasonable person”). Here, however, considering the language in the PSN User Agreement and the PSN Privacy Policy as a whole, it is entirely plausible that a reasonable consumer might have been deceived by Sony’s representations of reasonable security, industry-standard encryption, and the corresponding disclaimer of perfect security.

Accordingly, because Plaintiffs have alleged that Sony’s network security is still inadequate, the Court DENIES Sony’s motion to dismiss the injunctive and declaratory relief claims under the MCPA. (FACC ¶ 285) (“Defendants continue to misrepresent the adequacy of their security systems and will continue to so unless retained by Court order.”).

4. **Missouri Merchandising Practices Act**

Count 22 is brought by Plaintiff Munsterman and alleges violation of the MMPA. (FACC ¶¶ 314-328.) The MMPA was enacted “to preserve fundamental honesty, fair play, and right dealings in public transactions,” *Scott v. Blue Springs Ford Sales, Inc.*, 215 S.W.3d 145, 160 (Mo. Ct. App. 2006), and prohibits “deception, fraud, false pretense, false promise, misrepresentation, unfair practice or concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce.” Mo. Rev. Stat. § 407.020(1). To state a claim under the MMPA, a plaintiff must allege: (1) the purchase of merchandise; (2) for
personal, family, or household purposes; and (3) an ascertainable loss of money or property as a result of an act or practice declared unlawful under the MMPA. See Hess v. Chase Manhattan Bank, USA, N.A., 220 S.W.3d 758, 773 (Mo. 2007); Owen v. Gen. Motors Corp., 533 F.3d 913, 922 (8th Cir. 2008) (stating that the MMPA requires a casual connection between the ascertainable loss and the alleged unfair or deceptive practice). The MMPA defines merchandise as “objects, wares, goods, commodities, intangibles, real estate or services.” Edmonds v. Hough, 344 S.W.3d 219, 223 (Mo. Ct. App. 2011), reh'g and/or transfer denied (May 24, 2011), transfer denied (Aug. 30, 2011); Mo. Rev. Stat. § 407.010(4).

Plaintiffs allege Sony violated the MMPA by “failing to disclose that the security of Plaintiffs’ Personal Information on Sony Online Services was inadequate,” and that Sony had a “legal duty” to disclose this information to consumers. (FACC ¶ 320-321.) Sony moves to the dismiss the MMPA claim on the basis that Plaintiffs have failed to allege: (1) an ascertainable loss of money or property caused by Sony’s alleged misconduct; (2) the purchase or lease of merchandise; (3) a deceptive or unfair practice; and (4) an entitlement to declaratory or injunctive relief. The Court disagrees.

As a general matter, Sony erroneously characterizes the MMPA claim as one based solely on affirmative misrepresentations, rather than a claim based on misrepresentations and omissions—an error fatal to most if not all of Sony’s contentions. Therefore, although Sony argues that Plaintiffs have not alleged the purchase of merchandise flowing from a violation of the MMPA, because Plaintiffs purchased their Consoles prior to being presented with the alleged misrepresentations, Sony’s arguments fail to account for Plaintiffs’ allegations that Sony omitted material information regarding the security of its network at the point of sale of the Consoles. Thus, the Court finds Plaintiffs have sufficiently alleged that Plaintiff Munsterman would not have purchased his Console if Sony had disclosed the truth regarding the security of its network. See Sunset Pools of St. Louis, Inc. v. Schaefer, 869 S.W.2d 883, 886 (Mo. Ct. App. 1994) (“Courts of this
state apply the benefit of the bargain rule to determine the damages in cases of fraud or deceit where the parties have not elected to rescind the contract and seek restitution.”).

Next, the parties dispute whether Plaintiffs have alleged an ascertainable loss of money or property as a result of an act or practice declared unlawful under the MMPA. Mo. Rev. Stat. § 407.020 (stating that an act is deemed unlawful if it is unfair or deceptive). Similar to Sony’s first contention, however, this dispute is easily dispelled. Plaintiffs’ MMPA claim is premised in part on Sony’s alleged material omissions regarding the security of its network, omissions that allegedly induced Plaintiffs to purchase their Consoles. See Owen, 533 F.3d at 922 (stating that MMPA claims can be based on material omissions); Hess, 220 S.W.3d at 774 (“Proof of omission or concealment of a material fact under the [MMPA] . . . plainly requires less proof than was required to prove the comparable elements of . . . common law fraud claim.”). Thus, because Plaintiffs have alleged that Sony’s omissions were deceptive and/or unfair because Sony misled consumers into believing that their Personal Information was secure, the Court finds Plaintiffs have sufficiently alleged a loss of money or property as a result of an act or practice declared unlawful under the MMPA. See, e.g., Ward v. W. Cnty. Motor Co., 403 S.W.3d 82, 84 (Mo. 2013).46

Finally, although Sony argues that Plaintiffs may not pursue equitable relief under the MMPA because they have not suffered actual damage, as stated above, this contention lacks merit. See Mo. Ann. Stat. § 407.025; Freeman Health Sys. v. Wass, 124 S.W.3d 504, 509 (Mo. Ct. App. 2004) (stating that “only after a claimant has successfully brought suit for actual damages under section 407.025, may the court consider awarding attorney’s fees, punitive damages, and other ‘equitable relief.’ ”). Accordingly, the Court DENIES Sony’s motion to dismiss the MMPA.

46 Sony reliance on Padberg v. DISH Network LLC, No. 11-04035-CV-C-NKL, 2012 WL 2120765 (W.D. Mo. June 11, 2012) is unavailing. The court in Padberg found no causation because the deception was remedied by express terms in the contract. Padberg, 2012 WL 2120765, at *5–6. Here, however, the language of the PSN User Agreement is potentially deceptive because Sony warranted “reasonable security” and “industry-standard encryption.” To the extent Sony did not utilize reasonable security the disclaimer of “perfect disclaimer” is potentially deceptive.
5. New Hampshire Consumer Protection Act

Count 28 is brought by Plaintiff Kallad and alleges violation of the NHCPA. (FACC ¶¶ 361-370.) The NHCPA prohibits the use of “any unfair or deceptive act or practice in the conduct of any trade or commerce.” N.H. Rev. Stat. § 358–A:2. Similar to the CLRA, the NHCPA provides a non-exhaustive list of prohibited practices, including several prohibitions codifying common law unfair competition. See N.H. Rev. Stat. § 358–A:2(II) (“Causing likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services”); N.H. Rev. Stat. § 358–A:2(III) (“Causing likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services”); N.H. Rev. Stat. § 358–A:2(V) (“Representing that goods or services have sponsorship [or] . . . approval that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that he does not have”). However, regardless of whether a practice is included in the NHCPA’s enumerated unlawful practices, conduct can violate the NHCPA if it “attain[s] a level of rascality that would raise an eyebrow of someone inured to the rough and tumble of the world of commerce.” Barrows v. Boles, 687 A.2d 979, 986 (N.H. 1996).

Plaintiffs allege Sony violated the NHCPA by misrepresenting the adequacy of Sony’s network security and by representing that PS3s, PSPs, and Sony Online Services had specific security characteristics, uses, and benefits, when Sony knew they did not. (FACC ¶¶ 366, 370.) Plaintiffs allege they suffered actual and statutory damages as a result of Sony’s deceptive conduct because the misrepresentations induced them to purchase their Consoles and/or register for Sony Online Services. (Id. at ¶ 367.) Plaintiffs also seek declaratory and injunctive relief under Section 358-A:10. (Id. at ¶ 369.) Sony moves to dismiss the NHCPA claim on the basis that Plaintiffs have failed to allege: (1) actual damages under Section 358-A:10-a(I); (2) unfair conduct; (3) causation; and (4) any basis for injunctive relief. The Court discusses each in turn.
First, contrary to Sony’s contentions, the NHCPA “does not require a showing of actual damages for the claimant to be awarded the statutory minimum and attorneys’ fees.” *Becksted v. Nadeau*, 926 A.2d 819, 824 (N.H. 2007); N.H. Rev. Stat. § 358–A:10(I).\(^{47}\) This principle is well established by New Hampshire’s highest courts and will not be disrupted here. *See, e.g.*, *Carter v. Lachance*, 766 A.2d 717, 720 (N.H. 2001) (stating that “[t]he statutory minimum award of $1,000 is not based upon actual damages suffered, but is a penalty imposed upon” those who violate the statute); *Becksted v. Nadeau*, 926 A.2d 819, 824 (N.H. 2007) (“Contrary to the trial court’s ruling, we have previously held that RSA § A:10 does not require a showing of actual damages for the claimant to be awarded the statutory minimum and attorney’s fees.”). Accordingly, as stated below, because the Court finds Plaintiffs have stated a plausible claim under the NHCPA, the Court DENIES Sony’s motion to dismiss the NHCPA claim seeking statutory damages.

Second, Sony contends Plaintiffs have failed to allege unlawful conduct under the NHCPA. As set forth in the FACC, Plaintiffs allege Sony violated three of the fourteen enumerated unfair or deceptive practices outlined in the NHCPA. These include:

V. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that such person does not have;

VII. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

IX. Advertising goods or services with intent not to sell them as advertised.

N.H. Rev. Stat. § 358–A:2(V), (VII), (IX). In addition to the enumerated provisions set forth above, Plaintiffs allege Sony’s violated the NHCPA because Sony’s conduct violated the “rascality test.” In opposition, Sony contends none of these allegations set forth a plausible claim for relief because no reasonable consumer would have been

\(^{47}\) “Any person injured by another’s use of any method, act or practice declared unlawful under this chapter may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper.” N.H. Rev. Stat. § 358–A:10(I).
deceived by Sony’s representations regarding “reasonable security.” In addition, to the
degree Plaintiffs base their NHCPA claim on acts or practices not specifically enumer-
“attain[s] a level of rascality that would raise an eyebrow,” or that Sony had the required
“State v. Moran, 861 A.2d 763, 765 (N.H. 2004). At this
As stated by the New Hampshire Supreme Court in Beer v. Bennett, 993 A.2d 765,
768 (N.H. 2010) “even if [] individual representations could be read as literally true, [an]
allegation could still violate the [NHCPA] if it created an overall misleading impres-
performance,” when in fact, the car was inoperable due to a number of missing parts. Id. In
affirming the trial court’s ruling, the New Hampshire Supreme Court noted that the
defendant’s conduct met the “rascality test, and therefore violated the NHCPA,” because
the defendant “made representations [] knowing that he lacked sufficient knowledge to
Here, Plaintiffs allege Sony affirmatively represented that it would take “reason-
know that its security systems were both inadequate and vulnerable to attack. Therefore,
in contrast to the cases cited by Sony, which contained clear disclaimers of the alleged
misrepresentations, at this stage in the proceedings, the Court cannot find that the
language in the PSN User Agreement and/or the PSN Privacy Policy did not create an
“overall misleading” impression as a matter of law. Beer, 993 A.2d at 768; Cf. Davis
22, 2006) (finding no violation of the NHCPA because contract disclosed that customers
might have to pay the full cost); L’Esperance v. HSBC Consumer Lending, Inc., No.
Third, Sony argues Plaintiffs’ class action allegations should be dismissed because Plaintiffs have not alleged an injury to unnamed class members that was “caused by” Sony’s deceptive or unlawful conduct. Sony relies on N.H. Rev. Stat. Section 358-A:10-a(I) to support this proposition. Under N.H. Rev. Stat. Section 358-A:10-a(I):

Persons entitled to bring an action under RSA 358-A:10 may, if the unlawful act or practice has caused similar injury to numerous other persons, institute an action as representative or representatives of a class of persons who are residents of this state or whose cause of action arose within this state against one or more defendants as individuals or as representatives of a class or against one or more such defendants having a principal place of business within this state, and the petition shall allege such facts as will show that these persons or the named defendants specifically named and served with process have been fairly chosen and adequately and fairly represent the whole class, to recover actual damages as provided for in RSA 358-A:10.

Based on the language of Section 358-A:10-a(I) and Section 358-A:10(I), which provide for the recovery of “actual damages or $1,000,” Sony contends statutory damages are disallowed in the absence of actual damages in the class action context. The Court agrees.

Although the New Hampshire Supreme Court has interpreted the NHCPA to allow plaintiffs to recover statutory damages in the absence of actual damages, the NHCPA still requires a named plaintiff instituting a representative action to allege that class members were personally harmed as a result of the defendant’s unlawful conduct. See Pagan v. Abbott Labs., Inc., 287 F.R.D. 139, 149 (E.D.N.Y. 2012) (“Nevertheless, the NHCPA still requires that the Plaintiffs show that the class members were personally harmed in some way by the Defendant’s unlawful conduct.”). Therefore, because Plaintiffs have failed to allege actual damages resulting from Sony’s alleged material misrepresentations, the Court GRANTS Sony’s motion to dismiss the class action.
allegations under the NHCPA without leave to amend. *See Birdsall v. Coolidge*, 93 U.S. 64, 64 (1876) (defining actual damages).\(^\text{48}\)

Finally, because the FACC seeks to enjoin Sony’s “wrongful acts and practices,” which includes Kalled’s individual allegations under the NHCPA that have not been dismissed, the Court DENIES Sony’s motion to dismiss Plaintiffs’ NHCPA claims seeking injunctive relief. N.H. Rev. Stat. § 358-A:10 (“Injunctive relief shall be available to private individuals under this chapter without bond, subject to the discretion of the court.”).

6. **New York Deceptive Practices Act**

Count 33 is brought by Plaintiff Whyland and alleges violation of the NYDPA.\(^\text{49}\) (FACC ¶¶ 393-403.) In order to state a claim under the NYDPA, “a plaintiff must show: (1) that the act, practice or advertisement was consumer-oriented; (2) that the act, practice or advertisement was misleading in a material respect; and (3) that the plaintiff was injured as a result of the deceptive practice, act or advertisement.” *Pelman v. McDonald's Corp.*, 237 F. Supp. 2d 512, 525 (S.D.N.Y. 2003); *see also* N.Y Gen. Bus. Law § 349 (“Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful.”). An act, practice, or advertisement is considered misleading if it is “likely to mislead a reasonable consumer acting reasonably under the circumstances.” *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank*, 85 N.Y.2d 20, 26 (N.Y. 1995).

Plaintiffs allege Sony violated the NYDPA by misleading consumers into believing that their Personal Information would be safe upon transmission to Sony, when Sony knew that its security systems were woefully inadequate. (FACC ¶ 397.) Plaintiffs

\(^\text{48}\) Plaintiffs have failed to allege actual damages under the NHCPA because they have not alleged material misrepresentations at or prior to the purchase of their Consoles, have not alleged actual instances of identify theft or unauthorized charges, and cannot recover damages relating to a brief interruption in PSN access because uninterrupted service was clearly disclaimed in the PSN User Agreement. (Doc. No. 94-2, Ex. A at 9.)

\(^\text{49}\) Count 33 only alleges a violation of Section 349 (Deceptive Acts and Practices) and not Section 350 (False Advertising).
allege they were injured as a result of these material misrepresentations because they: (1)
suffered a loss of privacy and/or a loss of value of their Personal Information; and (2)
paid for PSPs, PS3s, Sony Online Services and/or registered for Sony Online Services
after exposure to Sony’s materially misleading representations. *(Id. at ¶ 398.)* Sony
moves to dismiss the NYDPA claim on the basis that Plaintiffs have not alleged: (1)
actual injury caused by Sony’s material misrepresentations; (2) a deceptive act, practice,
or advertisement; and (3) any basis for injunctive relief. The Court finds Sony’s first
contention dispositive and therefore does not address the remaining grounds for dis-
alleged violation of the New York Consumer Protection Law . . . but it has not alleged
injury to consumers . . . and thus has not stated a claim under the statute.”).

With regard to damages, Sony contends Plaintiffs cannot state a claim under the
NYDPA because they have not alleged actual injury caused by Sony’s material misrepre-
sentations. Pursuant to Section 349(h), “any person who has been injured by reason of
any violation of this section may bring an action . . . to enjoin such unlawful act or
practice, an action to recover his actual damages or fifty dollars, whichever is great, or
both.” *N.Y. Gen. Bus. Law § 349(h).* New York courts interpreting this statutory
language have held that even though a plaintiff need not prove justifiable reliance on the
alleged deceptive conduct, a plaintiff must still allege “that the defendant engaged in a
material deceptive act or practice that caused actual, although not necessarily pecuniary
harm.” *Oswego Laborers' Local 214 Pension Fund, 647 N.E.2d at 745; see also Bose v.
Interclick, Inc.,* No. 10 CIV. 9183 DAB, 2011 WL 4343517, at *8–9 (S.D.N.Y. Aug. 17,
2011). Therefore, as further discussed below, although Plaintiffs attempt to plead actual
injury resulting from a loss of privacy and/or allegations that they purchased their
Consoles as a result of Sony’s material misrepresentations, neither is sufficient under
New York law.
First, with regard to Plaintiffs’ allegations that they suffered a loss of privacy and/or a loss in value of their Personal Information, each of cases relied upon by Plaintiffs are distinguishable. None of the cases dealt with a loss of privacy resulting from a data breach and each of the cases dealt with intentional conduct on behalf of the defendant. For example, in *Meyerson v. Prime Realty Sers., LLC*, 796 N.Y.S.2d 848, 851 (N.Y. App. Div. 2005), the court held that the plaintiff-tenant stated a viable claim against the defendant-landlord based on allegations that the landlord deceived the tenant into believing that the tenant had to disclose her Social Security Number prior to renewing her lease. Similarly, in *Anonymous v. CVS Corp.*, 728 N.Y.S.2d 333 (N.Y. App. Div. 2001), the court found that the plaintiffs had sufficiently alleged an injury under the NYDPA by alleging that the defendant pharmacy was intentionally disclosing the plaintiffs’ medical information without their consent. And finally, in *Bose v. Interclick, Inc.*, No. 10 CIV. 9183 DAB, 2011 WL 4343517, at *2 (S.D.N.Y. Aug. 17, 2011), the court found that an advertising company potentially violated the NYDPA because it used “flash cookies” and “history sniffing” to back up a user’s previously deleted cookies to intentionally track their browsing history. Therefore, even though each of these cases holds that an underlying privacy violation can form the basis of a NYDPA claim, none of these cases holds that information unintentionally disclosed by the defendant following a data breach is sufficient to state an injury under the NYDPA.

As a result, the Court finds the cases relied upon by Plaintiffs unavailing and the data breach cases cited by Sony highly instructive. See, e.g., *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007) (“Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.”); *Willey v. J.P. Morgan Chase, N.A.*, No. 09 CIV. 1397(CM), 2009 WL 1938987, at *9 (S.D. N.Y. July 7, 2009) (“The risk that plaintiff’s data may be misused because it has been lost is not a cognizable harm” under the NYDPA); *Shafran v. Harley-Davidson, Inc.*, No. 07 CIV. 01365 (GBD), 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008) (“Plaintiff’s alleged injuries are solely the result of a perceived and
speculative risk of future injury that may never occur.”); *Hammond v. The Bank of N.Y. Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *13 (S.D.N.Y. June 25, 2010) ("Thus, it is not surprising that the United States District Courts in New York, California, Illinois and Michigan (applying state law) have each found that the increased risk of identity theft (in the future) is not a cognizable claim."). Accordingly, although Plaintiffs allege that *Pisciotta, Willey, Shafran*, and *Hammond* are each distinguishable because they involved plaintiffs who alleged nothing more than an increased risk of identity theft rather than a loss of privacy, the Court does not agree. The plaintiffs in *Pisciotta, Willey, Shafran*, and *Hammond* each alleged a loss of privacy resulting from the disclosure of their personal information.

Second, Plaintiffs’ allegations that they were injured as a result of paying for their Consoles and/or registering for Sony Online Services are also without merit. (FACC ¶ 398.) As stated above, Plaintiffs’ misrepresentation allegations are based on representations contained within the PSN User Agreement and/or the PSN Privacy Policy, both of which were presented to Plaintiffs after they purchased their Consoles. Therefore, even though justifiable reliance is not required under the NYDPA, Plaintiffs cannot plausibly allege an injury relating to the purchase of their Consoles based on representations presented to Plaintiffs after they purchased their Consoles. *See Stutman v. Chem. Bank*, 95 N.Y.2d 24, 30 (N.Y. 2000) (requiring a causal link between the alleged injury and deceptive conduct). Moreover, even if Rule 9(b) does not apply to Plaintiffs’ NYDPA claim, Plaintiffs allegations that Sony’s conduct was deceptive must be based on Sony’s misrepresentations, and not purely on “reasonable consumer expectations.” (Doc. No. 164 at 26:9-12.) As a result, the Court finds Plaintiffs have failed to allege an injury based on the purchase price of their Consoles (no causation), or an injury based on registration for Sony Online Services (a free service that clearly disclaimed any right to uninterrupted service), and that Plaintiffs only alleged injury is the alleged deceptive conduct itself, which New York courts have consistently rejected as insufficient under the NYDPA. *See Baron v. Pfizer, Inc.*, 840 N.Y.S.2d 445, 448 (N.Y. 2007).
Accordingly, because Plaintiffs have failed to allege an injury caused by a violation of the statute, the Court GRANTS Sony’s motion to dismiss the NYDPA claim. Because further amendment of this claim would be futile, the Court dismisses the claim without leave to amend. See McLaughlin v. Anderson, 962 F.2d 187, 195 (2d Cir. 1992) (finding not abuse of discretion for court to dismiss without leave to amend).

7. Ohio Consumer Protection Statutes

Plaintiffs assert two consumer protection claims under Ohio law: (1) violation of the OCSPA (Count 37); and (2) violation of the ODTPA (Count 38). (FACC ¶¶ 421-431.) Each is discussed in turn.

a. The Ohio Consumer Sales Practices Act

The OCSPA “prohibits unfair, deceptive, and unconscionable practices in consumer sales transactions,” and permits both individual claims and representative actions. Marrone v. Philip Morris USA, Inc., 850 N.E.2d 31, 33 (Ohio 2006) (citing Ohio Rev. Code §§ 1345.02, 1345.03); City of Findlay v. Hotels.com, 441 F. Supp. 2d 855, 862 (N.D. Ohio 2006). Under Section 1345.09(B), a consumer can bring a claim on behalf of a class if “the defendant’s alleged violation of the [OCSPA] is substantially similar to an act or practice previously declared to be deceptive by one of the methods identified in” § 1345.09(B). Marrone, 850 N.E.2d at 33. The requisite notice under Section 1345.09(B) must be in the form of: “(1) a rule adopted by the Ohio Attorney General; or (2) a judicial decision involving substantially similar conduct.” McKinney v. Bayer Corp., 744 F. Supp. 2d 733, 743 (N.D. Ohio 2010). After the Court requested supplemental briefing on the OCSPA claim, Plaintiffs conceded that they were unable to locate an act “substantially similar to an act or practice previously declared to be deceptive” by the Ohio Attorney General or an Ohio state court. (Doc. No. 164 at 26:16-25.) As a result, the Court GRANTS Sony’s motion to dismiss the OCSPA claim without leave to amend.

50 Plaintiffs did not address Sony’s contentions that injunctive relief under the NYDPA is disallowed in the absence of actual injury.
b. Ohio Deceptive Trade Practices Act

Count 38 alleges violation of the ODTPA. (FACC ¶¶ 426-431.) Sony moves to dismiss the ODTPA claim on the basis that the statute does not grant consumers standing to sue. Sony cites In re Oreck Corp. Halo Vacuum & Air Purifiers Marketing and Sales Practices Litigation, No. 12-CV-2317, 2012 WL 6062047, at *11 (C.D. Cal. Dec. 3, 2012), and Gascho v. Global Fitness Holdings, LLC, 863 F. Supp. 2d 677, 699 (S.D. Ohio 2012), to support this proposition, both of which held that only commercial entities have standing to sue under the ODTPA. Plaintiffs cite Bower v. International Business Machines, Inc., 495 F. Supp. 2d 837 (S.D. Ohio 2007), in opposition.

Although the parties have presented the Court with conflicting case law, Bower represents a minority position not followed by a majority of Ohio’s intermediate appellate courts. See In re Oreck Corp., 2012 WL 6062047, at *11 (“Ohio district courts have criticized and declined to follow the decision in Bower.”). Therefore, because the Ohio Supreme Court has not addressed whether consumers have standing to bring suit under the ODTPA, and the “vast majority of federal courts and all lower state courts to address the issue have concluded that relief under the [ODTPA] is not available to consumers,” the Court finds Plaintiffs lack standing under the ODTPA. Phillips v. Philip Morris Companies, 290 F.R.D. 476, 2013 WL 1182233, at *6 (N.D. Ohio 2013 Mar. 21, 2013); see also West v. Am. Tel. & Tel. Co., 311 U.S. 223, 237 (1940) (stating that the court must consider decisions of intermediate appellate state courts unless it is convinced by other persuasive data that the highest court of the state would decide otherwise); Robins v. Global Fitness Holdings, 838 F. Supp. 2d 631, 649–50 (N.D. Ohio 2012) (collecting cases and stating that the Bower opinion fails to acknowledge that Ohio courts look to the Lanham Act when adjudicating claims under the ODTPA); In re Porsche Cars N. Am., 880 F. Supp. 2d 801, 874–75 (S.D. Ohio 2012) (offering four different reasons for rejecting Bower). Accordingly, the Court GRANTS Sony’s motion to dismiss the ODTPA claim without leave to amend.
8. **Texas Deceptive Trade Practices Act**

Count 44 is brought by Plaintiff Wilson and alleges violation of the TDTPA. (FACC ¶¶ 457-466.) In order to state a claim under the TDTPA, the plaintiff must allege that: (1) he is a consumer; (2) the defendant engaged in false, misleading, or deceptive acts; and (3) that the defendant’s conduct was the producing cause of the plaintiff’s damages. See Tex. Bus. & Com. Code § 17.50(a); *Martin v. Ford Motor Co.*, 914 F. Supp. 1449 (S.D. Tex. 1996).

Plaintiffs contend Sony violated the TDTPA by misrepresenting the security of Sony Online Services, advertising Sony Online Services with the intent not to sell the services as warranted, breaching express and implied warranties, and engaging in unconscionable conduct. Plaintiffs allege they were injured as a result of Sony’s conduct because they purchased their Consoles and/or registered for Sony Online Services after exposure to the alleged misrepresentations. (Id. at ¶ 463.)

Sony moves to dismiss the TDTPA claim on the basis that Plaintiffs have failed to allege: (1) an actual injury caused by Sony’s conduct; (2) that Plaintiffs are consumers as defined under the TDTPA; (3) a violation of the statute; and (4) any right to injunctive and/or declaratory relief. (Doc. No. 163 at 26-30.) The Court finds Plaintiffs have failed to allege an actual injury caused by Sony’s unlawful conduct and therefore does not address Sony’s remaining contentions.

With respect to damages, Sony contends Plaintiffs have failed to allege an actual injury caused by Sony’s unlawful conduct. To prevail under the TDTPA, a plaintiff must prove that the defendant’s misrepresentation or unlawful conduct was the “producing cause of [his] economic damages or damages for mental anguish.” Tex. Bus. & Com. Code § 17.50(a); see also *Alexander v. Turtur & Assocs.*, 146 S.W.3d 113, 117 (Tex. 2004). Texas courts interpreting the statute have held that “producing cause” language requires the defendant’s act to be both the “cause-in-fact” and a “substantial factor” in

51 Plaintiffs’ opposition to Sony’s supplemental brief represented that their TDTPA claims were based only on misrepresentations and unconscionable conduct, and not on breach of warranty.
the plaintiff’s alleged injuries. See, e.g., *Main Place Custom Homes, Inc. v. Honaker*, 192 S.W.3d 604, 616 (Tex. App. 2006); *Prudential Ins. Co. v. Jefferson Assoc.s.,* 896 S.W.2d 156, 161 (Tex. 1995); *Union Pump Co. v. Allbritton*, 898 S.W.2d 773, 775 (Tex. 1995). Although there may be more than one producing cause, the plaintiff must show that the defendant’s conduct was a “contributing cause” of the plaintiff’s alleged injury. *Main Place Custom Homes*, 192 S.W.3d at 616. Where a plaintiff bases his claim on misrepresentations, the plaintiff must also allege that he relied on the defendant’s misrepresentations to his detriment. See *Tex. Bus. & Com. Code § 17.50(a)(1)(B).*

Here, the FACC alleges Plaintiff Wilson suffered actual injury as a result of Sony’s unlawful conduct because he purchased his Console and/or registered for Sony Online Services “after” exposure to Sony’s material misrepresentations. (FACC ¶ 463.) Plaintiffs attempted to bolster these allegations in their opposition to Sony’s supplemental brief by stating that in addition to the injuries stated above, they are also more vulnerable to cyber stalking/phishing, and lost access to Sony Online Services during the brief interruption in PSN access. However, neither of these allegations were pled in the FACC, and even if they were, they would not suffice under the TDTPA. See *N. Port Firefighters' Pension--Local Option Plan v. Temple-Inland, Inc.*, 936 F. Supp. 2d 722, 740 (N.D. Tex. 2013). As recognized by Sony and unrebutted by Plaintiffs, Texas does not allow a plaintiff to recover under the TDTPA for the mere risk of future identity theft or speculative injuries. See *Martin v. Home Depot USA, Inc.*, 369 F. Supp. 2d 887, 890 (W.D. Tex. 2005) (discussing the actual injury requirement); *Higbie Roth Const. Co. v. Houston Shell & Concrete*, 1 S.W.3d 808, 814 (Tex. App. 1999) (“[plaintiff] seeks compensation for future damages, possible loss of coverage, and possible additional damages. These damages are conjectural, uncertain, and therefore not actionable under the [TDTPA].”). As a result, the Court only addresses whether Plaintiffs have sufficiently pled an actual injury stemming from the purchase of their Consoles and/or registration for Sony Online Services.
First, with respect to Plaintiffs’ allegations that they suffered an actual injury in
the form of the purchase price of their Consoles, Plaintiffs are unable to satisfy the
causation requirement. Throughout the FACC, Plaintiffs concede that they purchased
their Consoles before registering for Sony Online Services, and that the alleged misrep-
resentations were contained in the PSN User Agreement and/or the PSN Privacy
Policy—two agreements Plaintiffs were required to assent to before registering for the
network and after purchasing their Consoles. As a result, it is factually impossible for
Sony’s alleged misrepresentations to have been the “producing cause” of Plaintiffs’
decision to purchase their Consoles. See Bartlett v. Schmidt, 33 S.W.3d 35, 39 (Tex.
App. 2000) (stating that “the plaintiff must show that there is some unbroken causal
connection between the allegedly deceptive act and the actual damages suffered”); Elliott
is not a producing cause cannot, as a matter of law, constitute a proximate cause.”).

Moreover, contrary to Plaintiffs’ contentions, whether a cause of action under the
TDTPA is based on misrepresentations or unconscionable conduct, the plaintiff is still
required to show that the defendant’s unlawful conduct was the “producing cause” of the
plaintiff’s injury. See Tex. Bus. & Com. Code § 17.50(a); Daugherty v. Jacobs, 187
S.W.3d 607, 616 (Tex. App. 2006) (“As with false, misleading, or deceptive acts, it is
not enough that consumers merely prove unconscionable action or course of action, they
must also prove those actions were the producing cause of actual damages.”). Therefore,
the Court finds Plaintiffs’ allegations of injury relating to the purchase of their Consoles
fails as a matter of law.\footnote{52}

Second, Wilson’s allegation that he suffered an actual injury because he registered
for Sony Online Services is also without merit. As stated above, registration and use of
Sony Online Services was free, and Wilson does not allege that he purchased premium

\footnote{52 Plaintiffs’ reliance on Pirozzi v. Apple, Inc., No. 12-CV-01529-JST, 2013 WL
4029067, at 36 (N.D. Cal. Aug. 5, 2013) is similarly unavailing. The plaintiff in Pirozzi
asserted claims under the UCL, FAL, CLRA only after having read the defendant’s
alleged misrepresentations.}
PSN services. Moreover, although not alleged in the FACC, to the extent Plaintiffs allege they were injured as a result of the brief interruption in PSN access, or the inability to access Third Party Services via their Consoles, Sony clearly disclaimed any right to uninterrupted and continuous PSN access. See Robinson v. Match.com, LLC, No. 3:10-CV-2651-L, 2012 WL 5007777, at *11 (N.D. Tex. Oct. 17, 2012) aff’d sub nom. Malsom v. Match.com, LLC., No. 12-11123, 2013 WL 5495666 (5th Cir. Oct. 3, 2013). Accordingly, the Court GRANTS Sony’s motion to dismiss the TDTPA claim on the basis that Plaintiffs cannot plausibly allege an actual injury.53 Because further amendment would be futile Sony’s motion is granted without leave to amend. See Bittinger v. Wells Fargo Bank NA, 744 F. Supp. 2d 619, 626 (S.D. Tex. 2010).

G. California Database Breach Act

Plaintiffs’ fourth cause of action alleges Sony violated the California Database Breach Act (“DBA”) by failing to notify Plaintiffs of the intrusion in the most expedient manner possible and without unreasonable delay. (FACC ¶¶ 186-195.) Plaintiffs seek injunctive relief, attorneys’ fees, and economic damages (fees incurred to obtain credit monitoring services, loss of use and value of Sony Online Services, loss of use and value of Third Party Services, and a diminution in value of their Consoles) as a result of the violation. (Id. at ¶¶ 193-195.) Sony moves to dismiss the DBA claim on the basis that Plaintiffs have failed to allege: (1) why notice of the intrusion within the 90-day safe harbor provision set forth in Section 1798.84(d) was unreasonable; (2) how Sony’s conduct was willful, intentional, and/or reckless in violation of Section 1798.83; and (3) how Plaintiffs’ economic damages flow from the purported unreasonable delay.

California Civil Code Section 1798.82 sets forth the parameters of the DBA, including what is required to state a violation of the statute. In pertinent part, Section 1798.82 states:

________________________________________________________________________

53 Injunctive and declaratory relief are only available in the event the plaintiff prevails. Tex. Bus. & Com. Code § 17.50(b)(2) (“In a suit filed under this section, each consumer who prevails may obtain. . . an order enjoining such acts or failure to act”).
Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Cal. Civ. Code § 1798.82(a). Here, neither party contests that Sony conducts business in California, that Sony owns/licenses computerized data that includes Plaintiffs’ Personal Information, and that Plaintiffs’ Personal Information may have been exposed as a result of the intrusion. Therefore, in order to comply with the DBA, Sony was required to notify consumers of the intrusion “in the most expedient time possible and without unreasonable delay.” Id. Although Sony contends they complied with the DBA based on the 90-day safe harbor provision set forth in Section 1798.83(d), as correctly noted by Plaintiffs, the safe harbor provision only applies to the sale of information to marketers without disclosure, and is therefore inapplicable here. As a result, whether or not the ten-day delay was unreasonable is a factual determination not properly decided by the Court on a motion to dismiss.

Nonetheless, even though the length of the delay is a factual question to be resolved by the trier of fact, whether Plaintiffs have sufficiently pled an entitlement to damages or injunctive relief is a legal question to be determined by the Court. With respect to the recovery of actual damages, Section 1798.84(b) states that “[a]ny customer injured by a violation of this title may institute a civil action to recover damages.” Although case law interpreting Section 1798.84(b) is limited, unreported California cases and courts in other jurisdictions analyzing statutes mirroring the DBA have held that a plaintiff must allege actual damages flowing from the unreasonable delay (and not just the intrusion itself) in order to recover actual damages. See, e.g., Boorstein v. Men’s Journal, LLC, No. CV12-771 DSF (Ex), 2012 WL 2152815, at *2 (C.D. Cal. June 14,
2012); *Grigsby v. Valve Corp.*, No. 2:12-CV-00553-JLR, at *1–2 (Mar. 18, 2013) (“*Grigsby II*”).

For example, in *Grigsby II*, an unreported case out of the Western District of Washington, the court concluded that the words “injured by a violation” required the plaintiff to allege that the damages flowed from the delay, and not just that the damage flowed from the intrusion. (Doc. No. 146, Ex. A.) In pertinent part, the *Grigsby II* court stated:

Valve argues that Mr. Grigsby’s allegations concerning injury are insufficient. The court agrees. With respect to a claim under RCW 19.255.010, it is not enough for Mr. Grigsby to have been injured by the hacking incident. The statute does not penalize companies that simply suffer a security breach or fail to prevent an unauthorized third-party from acquiring their customers’ personal information; rather, the statute penalizes companies that fail to disclose such incidents in the manner prescribed by the statute to affected state residents. *See* RCW 19.255.010(1); *see also* RCW 19.255.101(10) (providing for a private right of action and injunctive relief). Thus, Mr. Grigsby must allege facts supporting the claim that he was injured due to the interval between the hacking incident and Valve’s notice of the incident and not just that he was injured by the hacking incident alone. Mr. Grigsby has failed to do so, and the court therefore finds his claim lacking in this respect as well.

(Doc. No. 146, Ex. A at 12:6-17.) The same conclusion can be reached in the instant case. Here, Plaintiffs have failed to allege how the ten-day delay caused Howe to incur expenses for credit monitoring services, when these credit monitoring services were purchased, how the loss of use and value of Sony Online Services and Third Party Services were caused by the delay (and not the intrusion), and how Plaintiffs’ Consoles diminished in value as a result of the delay.

Accordingly, the Court GRANTS Sony’s motion to dismiss the DBA claims seeking economic damages under § 1789.84(b). However, because Plaintiffs may pursue their injunctive relief claims under § 1798.84(e), which affords relief when a “business

---

54 In *Boorstein v. Men’s Journal*, the plaintiff brought a claim under the DBA alleging that the defendant failed to provide him with the required disclosures when it sold him a magazine. 2012 WL 2152815, at *1–5. The court dismissed the claim for failure to allege that the plaintiff suffered an injury as a result of the violation. *Id.*

*Grigsby II* is an unreported case attached as Exhibit A to Doc. No. 146.

55 The Washington statute mirrors the DBA.
violates, proposes to violate, or has violated” the DBA, the Court DENIES Sony’s motion to dismiss the DBA claim seeking injunctive relief.

**H. Violation of the Federal Fair Credit Reporting Act**

Plaintiffs assert two causes of action under the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 (“FCRA”). Count 49 alleges willful violation of the FCRA and Count 50 alleges negligent violation of the FCRA. (FACC ¶¶ 489-498, 499-504.) Sony moves to dismiss both claims on the basis that: (1) Defendants are not consumer reporting agencies as defined under the Section 1681a(f); and (2) Plaintiffs have failed to allege a plausible basis for relief. The Court finds Sony’s first contention dispositive.

**1. Consumer Reporting Agencies**

First, Sony contends Plaintiffs’ FCRA claims should be dismissed because Plaintiffs have not alleged which Defendants are consumer reporting agencies or how any of the Defendants fit the definition of a consumer reporting agency. Although Plaintiffs attempt to combat Sony’s contentions by arguing that each Defendant is a consumer reporting agency because they assembled the personal information of consumers for the purpose of furnishing information to third parties, including, by and between the various Sony Defendants, Plaintiffs’ allegations stretch the statutory definition beyond its plain meaning.

Congress enacted the FCRA to regulate “consumer reporting agencies” that accumulate consumer credit histories and then regularly make that information available to third parties via “consumer reports.” *Holmes v. Countrywide Fin. Corp.*, No. 08-CV-00205, 2012 WL 2873892, at *15 (W.D. Ky. July 12, 2012) (citing 15 U.S.C. § 1681). As defined by the FCRA, a “consumer reporting agency” is:

[A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which

56 Neither party addressed the Court’s tentative ruling at oral argument, which stated that both FCRA claims were subject to dismissal without leave to amend because none of the Defendants are “consumer reporting agencies” as defined under Section 1681a(f). (Doc. No. 157.)
uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f). Courts construing Section 1681a(f) have restricted the definition of “consumer reporting agency” to include only those agencies that furnish “consumer reports” for “consumer purposes.” Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *13 (N.D. Ga. Feb. 5, 2013) (recommending dismissal of FCRA claims in a data breach case where the plaintiffs failed to demonstrate that the defendant met the definition of a “consumer reporting agency” under the statute).

As a result, entities that utilize consumer reports for “business, commercial[,] or professional purposes” are not considered consumer reporting agencies under the FCRA. McCready v. eBay, Inc., 453 F.3d 882, 889 (7th Cir. 2006) (quoting Ippolito v. WNS, Inc., 864 F.2d 440, 452 (7th Cir. 1988)); FTC v. Gill, 265 F.3d 944, 948 (9th Cir. 2001) (“Consumer reporting agencies [under the FCRA] . . . like Trans Union, Experian, and Equifax must exercise care in accurately and completely reporting credit information.”); 15 U.S.C. § 1681a(d)(1).

Here, the FACC does not contain any allegations suggesting that Sony regularly compiles and distributes consumer reports as defined under the FCRA. Rather, Plaintiffs merely recite the language of the statute in an attempt to come within the confines of the FCRA, or stretch the statutory language beyond its intended purpose. For example, although Plaintiffs allege that Sony furnished reports to “third parties” by disseminating Plaintiffs’ Personal Information by and between the Sony Defendants, such conduct is clearly excluded under the FCRA when it occurs between entities related by common ownership. See 15 U.S.C. § 1681a(d)(2)(ii) (excluding from the definition of “consumer report” any communication of transaction information “among persons related by common ownership or affiliated by corporate control”). Moreover, to the extent Plaintiffs attempt to allege that their Personal Information was furnished to third parties...
as a result of the intrusion, this argument has also been rejected.\textsuperscript{57} See, e.g., Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *13 (N.D. Ga. Feb. 5, 2013); Holmes, 2012 WL 2873892, at *16 (“No coherent understanding of the words “furnished” or “transmitted” would implicate Countrywide’s action under the FCRA.”). Accordingly, the Court GRANTS Sony’s motion to dismiss both FCRA claims without leave to amend.

\textbf{I. Partial Performance and Breach of the Covenant of Good Faith and Fair Dealing}

Plaintiffs’ final cause of action seeks partial performance and breach of the covenant of good faith and fair dealing regarding a settlement agreement (“Settlement Agreement”) allegedly entered into by and between Sony and Plaintiffs’ counsel. (FACC ¶¶ 505-515.) Plaintiffs allege the Settlement Agreement was entered into between the parties soon after the instant litigation commenced, and required the parties to negotiate attorney’s fees, costs, and expenses, in addition to including the Canadian and Israeli cases in the settlement. (\textit{Id.} at ¶¶ 506, 509.) Plaintiffs allege that after the Canadian cases joined in the Settlement Agreement and Sony waived the requirement that the Israeli cases join, Sony failed to negotiate attorney’s fees, costs, and expenses with Plaintiffs and separately settled with the Canadian plaintiffs. (\textit{Id.} at ¶¶ 510-512.) As a result, Plaintiffs seek partial performance of the Settlement Agreement, including attorney’s fees, costs, and expenses incurred in the litigation thus far. (\textit{Id.} at ¶ 515.)

Sony moves to dismiss the claim on the basis that Plaintiffs confuse settlement discussions with an executed settlement agreement. Sony contends that because Plaintiffs do not allege facts showing that an agreement was in fact executed (and by whom), the date the agreement was allegedly executed, or that an executed agreement

\textsuperscript{57} The two cases cited by Plaintiffs are distinguishable. See, e.g., Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391, at *2–4 (N.D. Ill. Jan. 5, 2010) (stating that whether or not the defendant was a consumer reporting agency was not at issue); Ori v. Fifth Third Bank, 674 F. Supp. 2d 1095, 1097–98 (E.D. Wis. 2009) (finding that the defendant reseller was a consumer reporting agency under the FCRA based on a specific provision in the statute applying to resellers).
was ever delivered from one party to another, Plaintiffs have failed to state a viable cause of action. Moreover, to the extent that there was an actual settlement agreement executed between the parties, Sony contends the continued prosecution of this case is tantamount to an abandonment of the Settlement Agreement.58

Based on the arguments set forth above, the crux of the disagreement between the parties focuses on whether an executed agreement actually exists, and if it does not, the extent to which an “agreement to negotiate” can form the basis of Plaintiffs’ claim. Although the Court is perplexed as to why Plaintiffs did not file a motion to enforce the Settlement Agreement (to the extent there is an executed settlement agreement between the parties), Plaintiffs’ claim could be based on an alleged breach of an “agreement to negotiate.” As explained by the California Court of Appeal in Copeland v. Baskin Robbins USA, 96 Cal. App. 4th 1251, 1257, 1260 (Cal. Ct. App. 2002), which distinguished an agreement to agree (not actionable) from an agreement to negotiate (potentially actionable), a party can be liable based on an “agreement to negotiate” where the failure to reach an “ultimate agreement resulted from a breach of that party’s obligation to negotiate or to negotiate in good faith.” Here, Plaintiffs allege that the Settlement Agreement required the parties to negotiate attorney’s fees, costs, and expenses in good faith, and that Sony failed and refused to negotiate such expenses with Plaintiffs as required under the agreement. Plaintiffs further allege that Sony separately settled with the Canadian plaintiffs in direct contravention of the Settlement Agreement. Therefore, to the extent there is an executed document requiring Sony to negotiate attorney’s fees, costs, and expenses, and Sony failed to do so, or negotiated with Plaintiffs in bad faith, Plaintiffs have stated a claim for relief. Accordingly, at this stage in the proceedings, the Court DENIES Sony’s motion to dismiss Plaintiffs’ final cause of action alleging partial performance and breach of the implied covenant of good faith and fair dealing.

58 Neither party addressed the Court’s tentative ruling at oral argument, which stated that Plaintiffs’ partial performance/breach of the covenant of good faith and fair dealing claim was subject to dismissal with leave to amend. (Doc. No. 157.)
CONCLUSION

For the reasons set forth above, the Court GRANTS IN PART and DENIES IN PART Defendants’ motion to dismiss the FACC. (Doc. No. 135.) Defendants are instructed to file an answer to the FACC no later than **February 22, 2014**, and contact Magistrate Judge Dembin’s chambers to schedule a Case Management Conference and the necessary Rule 26 requirements no later than **February 4, 2014**. Accordingly, the following causes of action have been dismissed without leave to amend:

1. California Negligence Claim (Count 5);
2. Florida Negligence Claim (Count 11);
3. Massachusetts Negligence Claim (Count 14);
4. Missouri Negligence Claim (Count 27);
5. Ohio Negligence Claim (Count 43);
6. Florida Negligent Misrepresentation Claim (Count 9);
7. Massachusetts Negligent Misrepresentation Claim (Count 15);
8. Michigan Negligent Misrepresentation Claim (Count 19);
9. New Hampshire Negligent Misrepresentation Claim (Count 31);
10. Ohio Negligent Misrepresentation Claim (Count 42);
11. Texas Negligent Misrepresentation Claim (Count 47);
12. Michigan Innocent Misrepresentation Claim (Count 20);
13. Missouri Negligent Omission Claim (Count 26);
14. Florida Breach of Warranty Claim (Count 7);
15. Michigan Breach of Warranty Claim (Count 17);
16. Missouri Breach of Warranty Claim (Count 24);
17. New Hampshire Breach of Warranty Claim (Count 29);
18. New York Breach of Warranty Claim (Count 34);
19. Ohio Breach of Warranty Claims (Counts 40, 41);
20. Texas Breach of Warranty Claim (Count 45);
21. Florida Breach of Implied Warranty Claim (Count 8);
22. Michigan Breach of Implied Warranty Claim (Count 18);
23. Missouri Breach of Implied Warranty Claim (Count 25);
24. New York Implied Warranty Claim (Count 35);
25. Massachusetts Implied Warranty Claim (Count 12);
26. New Hampshire Implied Warranty Claim (Count 30);
27. Texas Implied Warranty Claim (Count 46);
28. Florida Unjust Enrichment Claim (Count 10);
29. Massachusetts Unjust Enrichment Claim (Count 13);
30. Michigan Unjust Enrichment Claim (Count 21);
31. Missouri Unjust Enrichment Claim (Count 23);
32. New Hampshire Unjust Enrichment Claim (Count 32);
33. New York Unjust Enrichment Claim (Count 36);
34. Ohio Unjust Enrichment Claim (Count 39);
35. Texas Unjust Enrichment Claim (Count 48);
36. UCL and FAL Claims based on misrepresentations regarding uninterrupted PSN and Internet access and Plaintiffs’ ability to seek injunctive relief (Counts 1, 2);
37. FDUTPA Claim seeking actual damages (Count 6);
38. MCPA Claim seeking actual damages (Count 16);
39. Class Action Claims under the NHCPA (Count 28);
40. NYDPA Claim (Count 33);
41. OCSPA Claim (Count 37);
42. ODTPA Claim (Count 38);
43. TDTPA Claim (Count 44);
44. DBA Claim seeking economic damages (Count 4); and
45. FCRA Claims (Counts 49, 50).

//
//
The following causes of action have survived dismissal and may proceed:

1. UCL and FAL Claims based on misrepresentations and omissions regarding reasonable network security and industry-standard encryption and Plaintiffs’ ability to seek restitution under the statutes (Counts 1, 2);

2. CLRA Claim based on misrepresentations and omissions regarding reasonable network security and industry-standard encryption;

3. FDUTPA Claim requesting declaratory and injunctive relief (Count 6);

4. MCPA Claim requesting declaratory and injunctive relief (Count 16);

5. MMPA Claim seeking damages and equitable relief (Count 22);

6. NHCPA Claim seeking damages and injunctive relief (Count 28);

7. DBA Claim requesting injunctive relief (Count 4);


IT IS SO ORDERED.

DATED: January 21, 2014

Hon. Anthony J. Battaglia
U.S. District Judge
In September 2011, a thief broke into a car sitting in a San Antonio parking garage and stole the car’s GPS system, stereo, and several data tapes. This seemingly run-of-the-mill theft has spawned massive litigation. Why? Because of the contents of those pilfered tapes. The car, as it turns out, belonged to an employee of Science Applications International Corporation, an information-technology company that handles data for the federal government. And the tapes contained personal information and medical records concerning 4.7 million members of the U.S. military (and their families) who were enrolled in TRICARE health care, which contracts with SAIC – somewhat ironically – to protect patients’ data.

Plaintiffs, who are potential victims of the data breach, filed a number of lawsuits in various courts around the country alleging harm from an increased likelihood of identity theft and from an invasion of their privacy, among other things. Eight of those suits have been consolidated here as a multi-district litigation. Recently, SAIC and the three Government Defendants – TRICARE, the Department of Defense, and its Secretary, Chuck Hagel – moved to dismiss the now-consolidated Complaint. Defendants claim that the service members can show
no injury based on the data breach and hence lack standing to sue in federal court; in addition, SAIC and the Government contend, none of the victims has stated a claim for relief under any of the many federal and state laws that might protect them. Plaintiffs rejoin that they have, in fact, been injured by the breach and that their various causes of action – ranging from state tort law to the federal Privacy Act of 1974 – are sound.

This case presents thorny standing issues regarding when, exactly, the loss or theft of something as abstract as data becomes a concrete injury. That is, when is a consumer actually harmed by a data breach – the moment data is lost or stolen, or only after the data has been accessed or used by a third party? As the issue has percolated through various courts, most have agreed that the mere loss of data – without evidence that it has been either viewed or misused – does not constitute an injury sufficient to confer standing. This Court agrees. Mere loss of the data is all that most Plaintiffs allege here, so the majority must be dismissed from this case. Two Plaintiffs, however, do plausibly assert that their data was accessed or abused, and those victims may move forward with their claims.

Standing thus resolved, the Court would typically next delve into the merits of the remaining Plaintiffs’ claims. In this case, however, the Court believes it more advisable to pause and confer with the litigants. The dismissal of most Plaintiffs will have serious consequences moving forward, which may well alter the parties’ perceptions of the case and how they prefer to proceed. Not every count in the Complaint applies to every Plaintiff, for example – so many of the counts may fall on that basis alone. Given that many of the Plaintiffs have been dismissed, moreover, they may desire to appeal immediately, which the Court might sanction. See Fed. R. Civ. P. 54(b). This matter was, after all, intended to proceed as a class action, and the number of potential class members has now considerably diminished. The Court will thus hold a status
hearing to assess the parties’ intentions before taking up the question of whether the two
remaining Plaintiffs have stated a legal claim.

I. Background

   A. Factual Background

   As outlined above, this case revolves around the theft of several data tapes from an SAIC
employee’s car in 2011. See Compl., ¶¶ 99-100. As the police report indicates, those tapes were
taken along with a GPS and stereo when a criminal smashed a window and broke into the vehicle
Compl., ¶ 100.1 Despite the efforts of law enforcement, the thief was never apprehended.

   The tapes were backup copies of medical data related to over 4 million TRICARE
beneficiaries who had received medical treatment or testing in San Antonio, Texas. See Compl.,
¶ 93. On September 29, 2011, TRICARE released a statement detailing the data breach to alert
customers to the situation. See id. In November, SAIC mailed letters to affected service
members explaining the scope of the theft and noting that “the information contained on the
tapes may include names, Social Security Numbers, addresses, dates of birth, phone numbers,”
and a variety of medical information. SAIC Mot., Exh. B (Letter from SAIC to Customer (Nov.
16, 2011)) at 1; see Compl., ¶ 94.2 But the tapes did not include “any financial data, such as
credit card or bank account information.” Letter from SAIC at 1. SAIC also observed, “The
chance that [any] information could be obtained from these tapes is low since accessing, viewing
and using the data requires specific hardware and software.” Id. SAIC nevertheless offered all

---

1 The police report is a public record subject to judicial notice. See Kaempe v. Myers, 367 F.3d 958, 965
(D.C. Cir. 2004). In addition, when a court considers jurisdictional arguments, it may rely on evidence outside of
the Complaint. See Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1253 (D.C. Cir. 2005).

2 The Letter from SAIC is incorporated by reference into the Consolidated Amended Complaint, which
relies on it heavily. See, e.g., Compl., ¶¶ 30-62, 114-17.
affected parties free credit monitoring and identity-theft protection and restoration services for one year. See id.

Still, Plaintiffs claim that the data breach caused them substantial harm. Twenty-four of the thirty-three Plaintiffs here allege that they have been injured because of the disclosure alone.³ They claim that, even if no one has yet used their personal information, they face an increased risk of identity theft, which they view as a distinct and palpable harm. See Compl., ¶¶ 20, 23. They also claim that the data breach violated their expectation of privacy, as codified in various statutes, state tort law, and possibly through contract. See id., ¶¶ 1, 20, 21, 24. In addition, five of those twenty-four Plaintiffs claim that they have spent time or money monitoring their credit or interfacing with their banks since the theft, and that their time and effort should be compensable.⁴

Six Plaintiffs also claim that someone used their credit cards or bank accounts without their authorization, although no one alleges that financial information was actually on the stolen tapes.⁵ One of those six additionally claims that loans have been opened in his name using his personal information – presumably including his social security number, name, date of birth, and address, all of which were on the backup tapes.⁶ Yet another Plaintiff alleges that she was harmed because her medical identity has disappeared.⁷ Finally, two Plaintiffs allege that they have received unwanted phone calls or “phishing” emails, and one of those Plaintiffs claims that marketers have information about her medical condition that they likely obtained from the tapes.⁸

---

³ Compl., ¶¶ 30 (Adcock), 31 (Arellano), 32 (Bacon), 33 (Bates), 34 (Biggerman), 36 (Deatrick), 37 (Erickson), 39 (Hartman), 42 (Johnson), 44 (Losack), 45 (Martin), 46 (Moss-McUmber), 47 (Miller), 50 (Newman), 51 (O’Hara-Epperly), 52 (Palmer), 53 (Peting), 54 (Pineirovigo), 55 (Reznikov), 56 (Richardson), 57 (Roe), 58 (Trower), 59 (Walters), 61 (Worrell).
⁴ Compl., ¶¶ 37 (Erickson), 44 (Losack), 52 (Palmer), 56 (Richardson), 59 (Walters).
⁵ Compl., ¶¶ 35 (Curtis), 38 (Gaffney), 40 (Hawk), 41 (Hernandez), 43 (Keller), 48 (Morelli).
⁶ Compl., ¶ 35 (Curtis).
⁷ Compl., ¶ 60 (Warner).
⁸ Compl., ¶¶ 49 (Moskowitz), 62 (Yarde).
Plaintiffs filed this lawsuit against TRICARE, which is a government agency that provides insurance coverage and health care to active-duty service members and their families, see 10 U.S.C. §§ 1074, 1076, 1079; 32 C.F.R. pt. 199; Compl., ¶ 3, and against the Department of Defense and its Secretary. The breach victims are also suing SAIC, a security firm that contracts with TRICARE to ensure the security of the personally identifiable information (PII) and protected health information (PHI) in its records. See Compl., ¶ 67.

In their Consolidated Amended Complaint, Plaintiffs allege no fewer than twenty separate causes of action, ranging from the violation of various federal statutes – such as the Privacy Act, the Fair Credit Reporting Act, and the Administrative Procedure Act – to the contravention of state statutes and common law – such as claims of negligence, breach of contract, and violation of various state consumer-protection laws. The injuries alleged include: (i) increased risk of identity theft, which Plaintiffs peg at 9.5 times their pre-theft risk; (ii) expenses incurred in mitigating the risk of identity theft; (iii) loss of privacy through the exposure of their personal information; (iv) loss of the value of their personal and medical information; (v) loss of the value of their insurance premiums, which should have been used to pay for proper security measures; (vi) SAIC’s failure to meet the requisite standard for data security; (vii) the lost right to truthful information about their data security; (viii) statutory (or liquidated) damages; and, in at least one case, (ix) actual identity theft. Compl., ¶¶ 20-23. The Court will address each theory of injury in turn as it analyzes the standing of Plaintiffs to proceed.

---

9 At the time this suit was filed, TRICARE was overseen by a group called Tricare Management Activity, which is the entity Plaintiffs originally sued. TMA has since been disestablished, and the Defense Health Agency has taken over TMA’s duties. See TMA, Defense Health Agency, http://www.tricare.mil/tma/ (last visited May 1, 2014). For ease, the Court refers to both TRICARE and its management agency jointly as TRICARE.
B. Procedural Background

This action encompasses eight separate cases filed in four different courts around the country. While most of those actions originated here in D.C., others were transferred from the Northern and Southern Districts of California as well as the Western District of Texas. See ECF No. 1 (Transfer Order) at 1-3. Consolidation of those cases for pretrial purposes took effect in June 2012, id., and in August of that year the Court held a hearing to sort out the administrative details of the newly combined multi-district litigation. See ECF No. 13 (Hearing Tr.) at 6. In October 2012, Plaintiffs filed a Consolidated Amended Complaint encompassing the allegations of thirty-three Plaintiffs from twenty-four states. See Compl., ¶¶ 1, 154. In November 2012, Defendants moved to dismiss all thirty-three Plaintiffs for lack of standing or, in the alternative, to dismiss each cause of action as unsupported by the factual allegations in the Complaint. Since that time, Plaintiffs have moved to supplement their pleadings, Defendants have filed multiple notices of supplemental authority, and the case has been reassigned from one judge to another.

Having recently taken the reins, this Court now addresses the first major issue raised by the Motions to Dismiss: standing.

II. Legal Standard

Because this Opinion addresses only Defendants’ jurisdictional arguments, Federal Rule of Civil Procedure 12(b)(1) provides the relevant legal standard.

In evaluating Defendants’ Motions to Dismiss, then, the Court must “treat the complaint’s factual allegations as true . . . and must grant plaintiff ‘the benefit of all inferences that can be derived from the facts alleged.’” Sparrow v. United Air Lines, Inc., 216 F.3d 1111, 1113 (D.C. Cir. 2000) (quoting Schuler v. United States, 617 F.2d 605, 608 (D.C. Cir. 1979)) (internal citation omitted); see also Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1253
This standard governs the Court’s considerations of Defendants’ Motions under both Rules 12(b)(1) and 12(b)(6). See Scheuer v. Rhodes, 416 U.S. 232, 236 (1974) (“in passing on a motion to dismiss, whether on the ground of lack of jurisdiction over the subject matter or for failure to state a cause of action, the allegations of the complaint should be construed favorably to the pleader”); Walker v. Jones, 733 F.2d 923, 925-26 (D.C. Cir. 1984) (same). The Court need not accept as true, however, “a legal conclusion couched as a factual allegation,” nor an inference unsupported by the facts set forth in the Complaint. Trudeau v. Fed. Trade Comm’n, 456 F.3d 178, 193 (D.C. Cir. 2006) (quoting Papasan v. Allain, 478 U.S. 265, 286 (1986)) (internal quotation marks omitted). In addition, the “complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009) (quoting Bell Atlantic Corp. v. Twombly, 550 U.S. 54, 570 (2007)).

To survive a motion to dismiss under Rule 12(b)(1), Plaintiffs bear the burden of proving that the Court has jurisdiction to hear their claims. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992); U.S. Ecology, Inc. v. U.S. Dep’t of Interior, 231 F.3d 20, 24 (D.C. Cir. 2000). A court has an “affirmative obligation to ensure that it is acting within the scope of its jurisdictional authority.” Grand Lodge of Fraternal Order of Police v. Ashcroft, 185 F. Supp. 2d 9, 13 (D.D.C. 2001). For this reason, “‘the [p]laintiff’s factual allegations in the complaint . . . will bear closer scrutiny in resolving a 12(b)(1) motion’ than in resolving a 12(b)(6) motion for failure to state a claim.” Id. at 13-14 (quoting 5A Charles A. Wright & Arthur R. Miller, Federal Practice and Procedure § 1350 (2d ed. 1987)) (alteration in original). Additionally, unlike with a motion to dismiss under Rule 12(b)(6), the Court “may consider materials outside the pleadings in deciding whether to grant a motion to dismiss for lack of jurisdiction.” Jerome Stevens

III. Analysis

Before examining the merits of any claim, courts must begin with questions of jurisdiction. See Fla. Audubon Soc’y v. Bentsen, 94 F.3d 658, 663 (D.C. Cir. 1996) (en banc). Plaintiffs’ first battle, then, is to prove that they have standing to pursue their claims. See Steel Co. v. Citizens for a Better Env’t, 523 U.S. 83, 93-95 (1998). That, as it turns out, is an uphill climb for all but two of the named Plaintiffs.

Article III of the Constitution limits the power of the federal judiciary to the resolution of “Cases” and “Controversies.” U.S. Const. art. III, § 2; see also Allen v. Wright, 468 U.S. 737, 750 (1984) (discussing the case-or-controversy requirement). Because “standing is an essential and unchanging part of the case-or-controversy requirement of Article III,” Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992), standing is a necessary “predicate to any exercise of [the Court’s] jurisdiction.” Fla. Audubon Soc’y, 94 F.3d at 663.

“Every plaintiff in federal court,” consequently, “bears the burden of establishing the three elements that make up the ‘irreducible constitutional minimum’ of Article III standing: injury-in-fact, causation, and redressability.” Dominguez v. UAL Corp., 666 F.3d 1359, 1362 (D.C. Cir. 2012) (quoting Lujan, 504 U.S. at 560-61). Even in the class-action context, all named Plaintiffs “must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.” Warth v. Seldin, 422 U.S. 490, 502 (1975) (emphasis added). Each element of standing must be pled or proven with the requisite “degree of evidence required at the successive stages of the litigation.” Lujan, 504 U.S. at 561. That is, at the motion-to-dismiss

A. Injury in Fact

The Court will examine each element of standing in turn, beginning with injury in fact. An injury in fact is “an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” Lujan, 504 U.S. at 560 (citations and internal quotation marks omitted). “Allegations of possible future injury do not satisfy the requirements of Art. III. A threatened injury must be certainly impending to constitute injury in fact.” Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (internal quotation marks omitted) (emphasis added).

The Supreme Court recently reviewed the contours of this requirement in Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013). There, plaintiffs – who were attorneys and human-rights, labor, legal, and media organizations who worked with foreign clients or sources – contended that they were likely to be targeted for surveillance under the Foreign Intelligence Surveillance Act. See id. at 1145-46. This, they claimed, would work them harm. As such, they had taken steps to keep conversations with their clients confidential at their own personal expense. See id. The Court held, however, that plaintiffs did not have an injury in fact because the threat of surveillance was too speculative. There were, the Court reasoned, simply too many “ifs” involved before an injury came to pass. The plaintiffs would be impacted by FISA only if
(1) the government decided to target communications involving their clients and (2) used the challenged FISA provision to do so, (3) the Foreign Intelligence Surveillance Court authorized the eavesdropping, (4) the government succeeded in picking up their targets’ phone calls or e-mails, and, finally, (5) the plaintiffs were involved in whatever communication the government intercepted. Id. at 1147-48. The Court concluded that such “a highly attenuated chain of possibilities[] does not satisfy the requirement that threatened injury must be certainly impending.” Id. at 1148; see also Whitmore, 495 U.S. at 156-57 (speculative to assume that petitioner would request federal habeas review; habeas would be granted; petitioner would be retried for his capital offense; and thus, on appeal from this new trial, petitioner would suffer due to a lack of data on similarly situated criminal defendants); O’Shea v. Littleton, 414 U.S. 488, 496-97 (1974) (injury speculative where plaintiff would need to violate the law, be arrested, and be tried before a specific magistrate judge to be harmed by the judge’s allegedly illegal courtroom practice); Los Angeles v. Lyons, 461 U.S. 95, 105-09 (1983) (injury conjectural or hypothetical where plaintiff would have to commit an illegal act, be arrested, and be subjected to a chokehold in the future for injury to occur).

The Court added, “Respondents’ contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm” was also “unavailing – because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” Clapper, 133 S. Ct. at 1151.

With those precepts in mind – that an injury must be present or certainly impending, that an attenuated chain of possibilities does not confer standing, and that plaintiffs cannot create
standing by taking steps to avoid an otherwise speculative harm – the Court turns to Plaintiffs’ allegations of injury here.

1. Increased Risk of Harm and Monitoring Costs

Plaintiffs begin by asserting that an increased risk of harm alone constitutes an injury sufficient to confer standing to sue. Due to the data breach, they claim that they are 9.5 times more likely than the average person to become victims of identity theft. Compl., ¶ 23. That increased risk, they maintain, in and of itself confers standing. But as Clapper makes clear, that is not true. The degree by which the risk of harm has increased is irrelevant – instead, the question is whether the harm is certainly impending. See also Public Citizen, Inc. v. Nat’l Highway Traffic Safety Admin., 489 F.3d 1279, 1297-98 (D.C. Cir. 2007) (“‘increased risk’ is” not by “itself [a] concrete, particularized, and actual injury for standing purposes” – harm must be “actual” or “imminent,” not merely “increased”).

Here, the relevant harm alleged is identity theft. A handful of Plaintiffs claims that they have suffered actual identity theft, and those Plaintiffs have clearly suffered an injury. At least twenty-four, however, allege only a risk of identity theft. See supra n.3. At this point, the likelihood that any individual Plaintiff will suffer harm remains entirely speculative. For identity theft to occur, after all, the following chain of events would have to transpire: First, the thief would have to recognize the tapes for what they were, instead of merely a minor addition to the GPS and stereo haul. Data tapes, after all, are not something an average computer user often encounters. The reader, for example, may not even be aware that some companies still use tapes – as opposed to hard drives, servers, or even CDs – to back up their data. See Disk or Tape Backup: Which is Best?, Backup For Servers, http://goo.gl/7JsXQF (last visited Apr. 28, 2014). Then, the criminal would have to find a tape reader and attach it to her computer. Next, she
would need to acquire software to upload the data from the tapes onto a computer – otherwise, tapes have to be slowly spooled through like cassettes for data to be read. Id. After that, portions of the data that are encrypted would have to be deciphered. See Compl., ¶ 95 (“a portion of the PII/PHI on the data tapes was encrypted”). Once the data was fully unencrypted, the crook would need to acquire a familiarity with TRICARE’s database format, which might require another round of special software. Finally, the larcenist would have to either misuse a particular Plaintiff’s name and social security number (out of 4.7 million TRICARE customers) or sell that Plaintiff’s data to a willing buyer who would then abuse it.

The vast majority of Plaintiffs has not alleged that any of those things have happened – because they cannot. Those events are entirely dependent on the actions of an unknown third party – namely, the thief. At this point, we do not know who she was, how much she knows about computers, or what she has done with the tapes. The tapes could be uploaded onto her computer and fully deciphered, or they could be lying in a landfill somewhere in Texas because she trashed them after achieving her main goal of boosting the car stereo and GPS. Unfortunately, there is simply no way to know until either the crook is apprehended or the data is actually used. Courts for this reason are reluctant to grant standing where the alleged future injury depends on the actions of an independent third party. See Clapper, 133 S. Ct. at 1150 (expressing “our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors”).

That is, no doubt, cold comfort to the millions of servicemen and women who must wait and watch their credit reports until something untoward occurs. After all, it is reasonable to fear the worst in the wake of such a theft, and it is understandably frustrating to know that the safety of your most personal information could be in danger. The Supreme Court, however, has held
that an “objectively reasonable likelihood” of harm is not enough to create standing, even if it is enough to engender some anxiety. See id., 133 S. Ct. at 1147-48. Plaintiffs thus do not have standing based on risk alone, even if their fears are rational.

Nor is the cost involved in preventing future harm enough to confer standing, even when such efforts are sensible. See id. at 1150-51. There is, after all, nothing unreasonable about monitoring your credit after a data breach. In fact, that is exactly what TRICARE and SAIC advised Plaintiffs to do – and what SAIC, in part, offered to pay for. See, e.g., Letter from SAIC at 1. But the Supreme Court has determined that proactive measures based on “fears of . . . future harm that is not certainly impending” do not create an injury in fact, even where such fears are not unfounded. Clapper, 133 S. Ct. at 1151. Put another way, the Court has held that plaintiffs cannot create standing by “inflicting harm on themselves” to ward off an otherwise speculative injury. Id. The cost of credit monitoring and other preventive measures, therefore, cannot create standing.

There is, however, an alternative argument. Plaintiffs point out that, in Clapper, the Court acknowledged that it sometimes “found standing based on a ‘substantial risk’ that . . . harm will occur, which [could] prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.” Clapper, 133 S. Ct. at 1150 n.5 (emphasis added). So Plaintiffs could, theoretically, prevail if the risk of harm here were substantial. Yet, Plaintiffs’ Complaint itself makes clear that they do not surmount that hurdle. To be sure, Plaintiffs allege that data-breach victims in general are 9.5 times more likely than the average person to experience identity theft post-breach. Compl., ¶ 132. But then Plaintiffs note that, overall, only about 19% of breach victims actually experience identity theft. Id. By Plaintiff’s own calculations, then, injury is likely not impending for over 80% of victims – and the figure is likely to be considerably higher in this
case, where the theft was unsophisticated and where the lack of widespread harm suggests that the tapes have not ever been accessed. Cf. Galaria, 2014 WL 689703, at *5. The harm in these circumstances, therefore, cannot satisfy the requirement of either the Supreme Court or the D.C. Circuit that there be “(i) a substantially increased risk of harm and (ii) a substantial probability of harm with that increase taken into account.” Public Citizen, Inc., 489 F.3d at 1295.

The conclusion that an increased risk of harm alone does not confer standing is supported by other courts’ analyses in similar data-breach cases. In Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), for example, a payroll company’s database was hacked, possibly exposing “employees’ names, addresses, social security numbers, dates of birth, and bank account information.” Id. at 40. Still, the Third Circuit held that, where it was “not known whether the hacker read, copied, or understood the data,” injury remained speculative. Id. In Randolph v. ING Life Insurance & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007), an unknown crook pilfered a laptop containing insurance information, including the “names, addresses, and Social Security numbers” of customers. Id. at 3. Nonetheless, because plaintiffs did “not allege that the burglar who stole the laptop did so in order to access their Information, or that their Information has actually been accessed since the laptop was stolen,” it was “mere speculation” to assume “that at some unspecified point in the indefinite future they w[ould] be the victims of identity theft.” Id. at 7-8; see also Whitaker v. HealthNet of Cal., Inc., No. 11-910, 2012 WL 174961, at *2 (E.D. Cal. Jan. 20, 2012) (“[P]laintiffs do not explain how the loss here has actually harmed them . . . or that third parties have accessed their data. Any harm stemming from their loss thus is precisely the type of conjectural and hypothetical harm that is insufficient to allege standing.”) (footnote omitted); Hammond v. Bank of N.Y. Mellon Corp., No. 08-6060, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) (“Plaintiffs lack standing” where backup data tapes were stolen.
and most plaintiffs alleged only a risk of harm “because their claims are future-oriented, hypothetical, and conjectural.”); Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010) (“Plaintiff’s alleged injury of an increased risk of identity theft is far too speculative.”); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1052 (E.D. Mo. 2009) (no standing where “plaintiff does not claim that his personal information has in fact been stolen and/or his identity compromised” in the data breach); Bell v. Acxiom Corp., No. 06-485, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (“[W]hile there have been several lawsuits alleging an increased risk of identity theft, no court has considered the risk itself to be damage. Only where the plaintiff has actually suffered identity theft has the court found that there were damages.”) (footnote omitted); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (In data-breach case, “plaintiff’s allegations, if true, create only the possibility of harm at a future date. Plaintiff] alleges that her potential injury is contingent upon her information being obtained and then used by an unauthorized person for an unlawful purpose.”) (citation omitted); Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036, at *5 (D.N.J. July 31, 2006) (“Plaintiff only alleges a potential injury (identity theft) that is contingent on (1) Plaintiff’s information falling into the hands of an unauthorized person and (2) that person using such information for unlawful purposes to Plaintiff’s detriment.”).

Litigants’ cost-of-monitoring claims fared no better. See, e.g., Reilly, 664 F.3d at 46 (“Appellants’ alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more ‘actual’ injuries than the alleged ‘increased risk of injury’ which forms the basis for Appellants’ claims.”); Randolph, 486 F. Supp. 2d at 8 (The “argument that the time and money spent monitoring a plaintiff’s credit suffices to establish an
injury overlook[s] the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized.”) (internal quotation marks omitted).


Most cases that found standing in similar circumstances, however, were decided pre-Clapper or rely on pre-Clapper precedent and are, at best, thinly reasoned. For example, in Ruiz v. Gap, Inc., 380 Fed. Appx. 689 (9th Cir. 2010) (Gap III), the court stated that a “credible threat of harm is sufficient to constitute actual injury for standing purposes.” Id. at 691; see also, e.g., Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (“the possibility of future injury may be sufficient to confer standing on plaintiffs; threatened injury constitutes ‘injury in fact’”) (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 947 (9th Cir. 2002)); Pisciotta v. Old Nat’l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (standing because “the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious”). Yet after Clapper, Gap III’s “credible threat of harm” standard is clearly not supportable.

Indeed, since Clapper was handed down last year, courts have been even more emphatic in rejecting “increased risk” as a theory of standing in data-breach cases. As one court noted, after “Clapper, the mere fact that the risk has been increased does not suffice to establish standing.” Strautins v. Trustwave Holdings, Inc., No. 12-9115, 2014 WL 960816, at *4 (N.D. Ill. Mar. 12, 2014). After all, an increased risk or credible threat of impending harm is plainly
different from certainly impending harm, and certainly impending harm is what the Constitution and Clapper require. Clapper, 133 S. Ct. at 1148; see, e.g., Strautins, 2014 WL 960816, at *4 (deciding in light of Clapper that injury was speculative based “on a number of variables, such as whether their data was actually taken during the breach, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded”); Galaria, 2014 WL 689703, at *5 (noting the similarity to Clapper and holding that “[i]n this case, an increased risk of identity theft, identity fraud, medical fraud or phishing is not itself an injury-in-fact because Named Plaintiffs did not allege – or offer facts to make plausible – an allegation that such harm is ‘certainly impending’”); Polanco v. Omnicell, Inc., No. 13-1417, 2013 WL 6823265, at *14 (D.N.J. Dec. 26, 2013) (relying on Clapper and Reilly to conclude that mere loss of data, without misuse, is not “an injury sufficient to confer standing”); but see In re Sony Gaming Networks & Customer Data Sec. Breach Litigation, MDL No. 11-2258, 2014 WL 223677, at *9 (S.D. Cal. Jan. 21, 2014) (finding standing post-Clapper based on a “plausibly alleged . . . ‘credible threat’ of impending harm”).

In sum, increased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm. At least twenty-four of the thirty-three Plaintiffs in this case, then, must rely on an alternative theory of injury.

2. Privacy

Plaintiffs also allege that they have been injured because their privacy was invaded by the data breach. Yet this claim suffers from the same defects as Plaintiffs’ previous contention. For a person’s privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party. Existing case law and legislation support that common-sense intuition: If no one has viewed your private information (or is about to view it imminently), then your privacy has
not been violated. See, e.g., 5 C.F.R. § 297.102 (Under Privacy Act, “[d]isclosure means providing personal review of a record, or a copy thereof, to someone other than the data subject or the data subject’s authorized representative, parent, or legal guardian.”) (emphasis added); Walia v. Chertoff, No. 06-6587, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008) (“accessibility” is not the same as “active disclosure”); Schmidt v. Dep’t of Veterans Affairs, 218 F.R.D. 619, 630 (E.D. Wisc. 2003) (Disclosure is “the placing into the view of another information which was previously unknown,” requiring that information be “actually viewed.”); Harper v. United States, 423 F. Supp. 192, 197 (D.S.C. 1976) (Disclose means “the imparting of information which in itself has meaning and which was previously unknown to the person to whom it was imparted.”); Fairfax Hosp. v. Curtis, 492 S.E. 2d 642, 644 (Va. 1997) (violation where third party “possess[ed]” and “reviewed” records).

Here, the majority of Plaintiffs contend neither that their personal information has been viewed nor that their information has been exposed in a way that would facilitate easy, imminent access. As in the Third Circuit case Reilly, it would be speculative to assume that the thief “read, copied, or understood the data.” 664 F.3d at 40. As a result, no invasion of Plaintiffs’ privacy is imminent. See also Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012) (dismissing privacy claim for lack of standing where information had not been viewed by third party); Allison, 2010 WL 3719243 (no standing in data-breach case, even where claim involved invasion of privacy); Giordano, 2006 WL 2177036 (same); Strautins, 2014 WL 960816 (same); but see Galaria, 2014 WL 689703 (allowing standing for certain claims based only on invasion of privacy); Am. Fed’n of Gov’t Emps. v. Hawley, 543 F. Supp. 2d 44, 50 n.12 (D.D.C. 2008) (“emotional trauma alone is sufficient to qualify as an” injury “under Section 552a(g)(1)(D) of the Privacy Act”) (internal quotation marks and alterations omitted).
To be sure, the Supreme Court has intimated that disclosure of personally identifiable information alone, along with some attendant emotional distress, may constitute “injury enough to open the courthouse door” in privacy actions. Doe v. Chao, 540 U.S. 614, 624-25 (2004). But again, disclosure involves publication to a third party. In that case, Doe’s social security number had actually been published by the government on various documents “sent to groups of [workers’-compensation] claimants, their employers, and the lawyers involved in their cases.” Id. at 617. In other words, Doe’s information was actually exposed to dozens of readers. Here, by contrast, disclosure and access of Plaintiffs’ personal information is anything but certain. Rather, the information itself is locked inside tapes that require some expertise to open and decipher. Indeed, it is highly unlikely that the crook even understood what the tapes were, let alone had the wherewithal to access them or navigate her way to any one of the 4.7 million records contained therein. And until Plaintiffs can aver that their records have been viewed (or certainly will be viewed), any harm to their privacy remains speculative.

A few of the Plaintiffs here do allege that their data was used.10 Those Plaintiffs have at least claimed an injury to their privacy insofar as they allege that their data was accessed. The other Plaintiffs, however, are out of luck.

3. Loss of Value

Plaintiffs next contend that they were injured by the loss of two valuable assets. First, they argue that they lost the value of their personal and medical information, which could be “sold on the cyber black market for $14 to $25 per medical record.” Compl., ¶ 21. Second, they claim they forfeited the value of their insurance premiums, which should have been used to pay for better security. See id., ¶ 22.

---

10 Compl., ¶¶ 35 (Curtis), 38 (Gaffney), 40 (Hawk), 41 (Hernandez), 43 (Keller), 48 (Morelli), 49 (Moskowitz), 62 (Yarde).
As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss. Even if the service members did intend to sell their own data – something no one alleges – it is unclear whether or how the data has been devalued by the breach. For those reasons, Plaintiffs’ first theory of injury is unsuccessful.

Similarly, as to the value of their insurance premiums, Plaintiffs do not plausibly allege any actual loss. They allege that they were paying for “health and dental insurance” – and they do not claim that they were denied coverage or services in any way whatsoever. See id. To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing. They do not maintain, moreover, that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime. Put another way, Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid. Nothing in the Complaint makes a plausible case that Plaintiffs were cheated out of their premiums. As a result, no injury lies.

4. Legal Violations

Plaintiffs next set forth various legal violations that they claim create standing: They argue that SAIC failed to meet the requisite legal standards for data security; that SAIC and TRICARE violated their right to truthful information about their data; and that certain statutes, if violated, give them the right to automatic damages or payment. Standing, however, does not merely require a showing that the law has been violated, or that a statute will reward litigants in general upon showing of a violation. Rather, standing demands some form of injury – some
showing that the legal violation harmed you in particular, and that you are therefore an appropriate advocate in federal court.

As the Supreme Court “has repeatedly held . . .[,] an asserted right to have the [defendant] act in accordance with law is not sufficient, standing alone, to confer jurisdiction on a federal court.” Allen v. Wright, 468 U.S. 737, 754 (1984). Rather, the unlawful activity must work some harm on Plaintiffs.

In terms of the alleged contravention of security standards, Plaintiffs have not outlined any actual or imminent harm caused by that purported violation – aside from the theories the Court has already rejected. Plaintiffs, therefore, cannot acquire standing on that basis.

The same is true of the supposed deprivation of Plaintiff’s “right to truthful information about the security of their PII/PHI.” Opp. to SAIC at 7. No independent harm has flowed from that so-called deprivation. Of course, as Plaintiffs point out, denial of information alone can sometimes create an injury when statutes require disclosure. See Zivotofsky ex rel. Ari Z. v. Sec’y of State, 444 F.3d 614, 617-19 (D.C. Cir. 2006) (noting that violation of plaintiff’s right to documents under Freedom of Information Act can create standing). Here, however, Plaintiffs have failed to allege any actual deprivation of information, even assuming they have a right to it. First, they claim that they were deprived of information before TRICARE and SAIC notified them of the data breach. Any injury that might have occurred during that time, however, has been cured, since SAIC has now explained the extent of the breach to Plaintiffs in some detail, see Letter from SAIC at 1, and no one alleges any independent harm caused by the delay. Indeed, expedient notification of the data breach and its scope, along with certain required contact information, is all the relevant laws demand. See, e.g., Cal. Civ. Code § 1798.82; Or. Rev. Stat. Ann. § 646A.604(1)-(2). In addition, Plaintiffs claim that they have been deprived of
truthful information because SAIC “[c]ategoriz[ed] the risk of access” to their data “as ‘low’” in their letters notifying servicemen of the breach. Compl., ¶ 116. But that is, at best, a difference of opinion – Plaintiffs do not identify any actual facts that SAIC or TRICARE has withheld. As a result, Plaintiffs’ abstract assertion that their “right to truthful information” has been violated does not constitute an injury, since the facts in the complaint identify neither an actual deprivation nor any independent harm.

5. Actual Misuse

As noted above, Plaintiffs who claim that their information was, in fact, accessed and misused have alleged an actual injury. That injury, however, must still be linked to Defendants’ conduct.

B. Causation


To review the bidding: The majority of Plaintiffs in this case lack standing to sue because they failed to allege any cognizable injury. Six Plaintiffs, however, claim that their data was actually misused; one Plaintiff claims she has suffered medical fraud; and two claim that their privacy was invaded by phone calls and other solicitations from companies that may have accessed their medical records. Each of these three groups of Plaintiffs must be able to link their harm to the data breach.
1. **Identity Theft**

Six out of thirty-three Plaintiffs allege that their personal information was used for fraudulent purposes. *See supra n.5.* Five of those six claim only that unauthorized charges were made to their existing credit cards or debit cards, or that money was withdrawn from an existing bank account. But here’s the problem: No one alleges that credit-card, debit-card, or bank-account information was on the stolen tapes. *See, e.g.,* Letter from SAIC at 1 (tapes did not include “any financial data, such as credit card or bank account information”). To be sure, as Plaintiffs’ counsel noted at the Court’s August hearing, a criminal could obtain some of a victim’s personal information from a data breach and then go “phishing” to get the rest. *See* Hrg. Tr. at 45–46. That is, the crook could acquire a name and phone number and then make calls pretending to be a legitimate business asking for information like credit-card or bank-account numbers. Here, however, the identity-theft Plaintiffs have not alleged any phishing. Indeed, they proffer no plausible explanation for how the thief would have acquired their banking information. In a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud. *See* Kristin Finklea, Cong. Research Serv., R40599, Identity Theft: Trends and Issues 1 (2014), available at http://goo.gl/bCsTEg (10.2 million Americans, out of around 308.7 million total, experienced identity theft in 2010). As that information was not on the tapes, though, Plaintiffs cannot causally link it to the SAIC breach.

One Plaintiff, however – Robert Curtis, a Colorado resident – may have a case.¹¹ After the data breach, he received “letters in the mail from American Express,” among others,

---

¹¹ Plaintiffs have moved to supplement their factual allegations concerning Curtis. *See* ECF No. 41 (Motion for Leave to File Supplemental Pleadings). The Court grants that Motion here, although it notes that its
“thanking him for applying for loans” that he had never applied for. Compl., ¶ 35. To apply for such a loan, one would likely need a person’s name, address, date of birth, and social security number – exactly the sort of information that was on the tapes. Id., ¶ 7. The Court believes that this creates a sufficient causal link between the identity theft – which has hurt Curtis’s credit history, id., ¶ 35 – and the tape theft.

That said, the Court would be remiss if it did not note that Curtis also alleges a spate of identity theft that cannot plausibly be linked to the tapes. For example, he also complains that many of his existing accounts have been tampered with in seriously concerning and, no doubt, frustrating ways. Id. In one instance, Curtis’s bank notified him when “an individual in Mexico” called his bank asking for money “and knew Plaintiff Curtis’ account number, unlisted telephone number, address, date of birth and e-mail address, Social Security number and answers to the security questions.” ECF No. 43 (Reply to Motion to Supplement Pleadings), Exh. A (Supplement to Compl., ¶ 35) at 1. No one alleges, however, that the name of Curtis’s bank, his account number, his e-mail address, or the answers to his security questions were on the stolen tapes. He also claims that “individuals wired approximately $32,500 out of his credit union account.” Id. But again, he does not claim that the account information was on the tapes, although he does aver that he gave TRICARE his payment information at some point. Id. The inescapable conclusion is that Curtis has been subjected to another, more profound data breach involving his financial – not medical – records.

As a result, the fraudulent loan applications may also be linked to this other, more severe data breach and not the SAIC breach. At this point, however, the Court is willing to give Curtis

__________________________

conclusions regarding Curtis would be the same under both the original and the amended pleadings.
the benefit of the doubt, since there is at least a plausible connection between some of the harm he has suffered and the SAIC theft.

2. *Medical Fraud*

Another Plaintiff, Robin Warner, claims that she experienced medical fraud because her medical records no longer exist. Compl., ¶ 60. This is a striking allegation, but it cannot establish standing because only backup tapes were stolen from the SAIC employee’s car. Id., ¶ 6. Warner does not explain how the disappearance of her medical identity can be linked to the theft of tapes that contained only copies of her actual medical records. She has thus not carried her burden of alleging causation and hence has no standing.

3. *Privacy*

Two final Plaintiffs – in addition to Curtis, who has experienced similar woes – claim that their privacy has been invaded due to the data breach. Murray Moskowitz simply alleges that he “has received a number of unsolicited calls from telemarketers and scam artists.” Id., ¶ 49. He does not otherwise link the calls to the tapes, claim that the callers have personal or private information found on the tapes, or even allege that his phone number was unlisted and hence would have been difficult for marketers to locate absent the assistance of the data thief. Moskowitz seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls. His harm, consequently, cannot plausibly be linked to the tapes.

Dorothy Yarde, on the other hand, does allege a credible link to the data breach. She claims that her “telephone number is unlisted.” Id., ¶ 62. Still, after the theft, “she received numerous unsolicited telephone calls from insurance companies and other[s]” pitching “medical products and services . . . targeted at a specific medical condition listed in her medical records.” Id. (emphasis added). She had not received such calls in the past. Id. The fact that the callers
had Yarde’s unlisted phone number and medical diagnosis – both of which were on the tapes – suffices to create a causal link.

C. Redressability

The third and final element of standing is redressability, which requires that it “be ‘likely,’ as opposed to merely ‘speculative,’ that the” alleged “injury will be ‘redressed by a favorable decision.’” Lujan, 504 U.S. at 561 (citation omitted).

At this point, only two Plaintiffs remain: Curtis, who has alleged actual misuse of his social security number, and Yarde, who has alleged a privacy violation linked to her medical information. Both harms can be redressed, at least in part, by a monetary reward. Those two Plaintiffs – and only those two Plaintiffs – therefore have standing to sue.

* * *

A reasonable reader may still wonder: If Curtis and Yarde’s information was potentially accessed or misused, why not presume that the remaining Plaintiffs’ information will suffer the same fate? Indeed, other courts have allowed cases to move forward where some form of fraud had already taken place. For example, in Anderson v. Hannaford Bros., 659 F.3d 151 (1st Cir. 2011), the First Circuit declined to question the plaintiffs’ standing where 1,800 instances of credit- and debit-card fraud had already occurred and had been clearly linked to the data breach. Id. at 162-67. Similarly, in Pisciotta, the court allowed plaintiffs to proceed where “the scope and manner of access suggest[ed] that the intrusion was sophisticated, intentional and malicious,” and thus that the potential for harm was indeed substantial. 499 F.3d at 632.

The circumstances here, however, are starkly different. First, the theft from the SAIC employee’s car was a low-tech, garden-variety one. Any inference to the contrary is undermined by the snatching of the GPS and car stereo. This is hardly a black-ops caper. Second, while
Curtis and Yarde have alleged personalized injury sufficient to surmount a motion to dismiss under Rule 12(b)(1), there are no facts here that plausibly point to imminent, widespread harm. In fact, the link between Curtis and Yarde’s injuries and the data breach barely crosses the line from possible to plausible. Curtis, after all, was almost certainly the victim of another, more severe data breach, and that breach may well have been responsible for every instance of identity theft he alleges. It remains likely, in other words, that no one accessed his information from the tapes. Yarde’s harm may also stem from another source. For example, she might have bought specific medications related to her condition over the counter at the neighborhood drugstore or online. That information could have been sold to companies targeting such patients – no data breach necessary. At this stage, the Court simply acknowledges that the link between the data breach and Yarde and Curtis’s claims is plausible, even if it is very likely that their harm stems from another source.

The fact that Curtis and Yarde’s allegations are plausible, however, does not lead to the conclusion that wide-scale disclosure and misuse of all 4.7 million TRICARE customers’ data is plausibly “certainly impending.” Clapper, 133 S. Ct. at 1147. After all, as previously noted, roughly 3.3% of Americans will experience identity theft of some form, regardless of the source. See Finklea, Identity Theft: Trends and Issues, supra, at 1. So one would expect 3.3% of TRICARE’s customers to experience some type of identity theft, even if the tapes were never read or misused. To quantify that percentage, of the 4.7 million customers whose data was on the tapes, one would expect around 155,100 of them to experience identity fraud simply by virtue of living in America and engaging in commerce, even if the tapes had not been lost. Here, only six Plaintiffs allege some form of identity theft, and out of those six only Curtis offers any plausible link to the tapes. And Yarde is the only other Plaintiff – out of a population of 4.7
million – who has offered any evidence that someone may have accessed her medical or personal information.

Given those numbers, it would be entirely implausible to assume that a massive identity-theft scheme is currently in progress or is certainly impending. Indeed, given that thirty-four months have elapsed, either the malefactors are extraordinarily patient or no mining of the tapes has occurred. This is simply not a case where hundreds or thousands of instances of fraud have been linked to the data breach. See, e.g., Anderson, 659 F.3d at 162-67. Rather, as far as the Court is aware, only six instances of fraud have been reported, and only two customers can plausibly link either identity theft or privacy violations to the tapes’ loss. As such, only those two Plaintiffs whose harm is plausibly linked to the breach may move forward with their claims.

IV. Conclusion

Since the majority of Plaintiffs has been dismissed – potentially altering the scope of the remaining litigants’ claims moving forward – the Court will pause to confer with the parties before determining which, if any, of the Complaint’s twenty counts has been properly alleged. The Court thus reserves the issue of whether Defendants’ Rule 12(b)(6) Motions should be granted for a future date. It further notes that it expects the parties to confer before the forthcoming status to determine if they can reach some agreement on the next procedural steps in the case.

For the aforementioned reasons, the Court will grant in part and deny in part Defendants’ Motions to Dismiss. A separate Order consistent with this Opinion will be issued this day.

/s/ James E. Boasberg
JAMES E. BOASBERG
United States District Judge

Date: May 9, 2014
ORDER GRANTING, IN PART, 
AND DENYING, IN PART, 
MOTION TO DISMISS SECOND 
AMENDED COMPLAINT AND 
SETTING CASE MANAGEMENT 
CONFERENCE

No. 11-MD-02264 JSW

This matter comes before the Court upon consideration of the motion to dismiss filed by 
Defendant Google, Inc. (“Google”). The Court has considered the parties’ papers, relevant 
legal authority, and the record in this case, and it HEREBY GRANTS, IN PART, AND 
DENIES, IN PART, Google’s motion to dismiss.

BACKGROUND\(^1\)

Plaintiffs, Kendrick Cochran (“Mr. Cochran”), Nicholas Lawrence (“Mr. Lawrence”), 
Beverly Julia Levine Hillman-Seidner (“Ms. Hillman-Seidner”), Joan Smith (“Ms. Smith”), 
Phillip Hall (“Mr. Hall”), and Maritsa Urias (“Ms. Urias”) (collectively “Plaintiffs”) allege that 
Google “gained and allowed third parties to have unauthorized access to, and engaged in 
unauthorized use of,” their mobile devices, which use Google’s Android Operating System 
(“AOS”). (Docket No. 54, Second Amended Consolidated Class Action Complaint (“SACC”), 
\(\S\) 2; see also id. \(\S\) 35-46.)

\(^1\) A more detailed account of the facts underlying this dispute is set forth in the 
Court’s Order granting in part and denying in part the motion to dismiss the First Amended 
Class Action Complaint. In re Google Android Consumer Privacy Litig., 2013 WL 1283236, 
According to Plaintiffs, they each installed one or more of the following software applications (“Apps”) on their Android mobile devices: Foursquare; Groupon; Advanced Task Killer; Angry Birds; and Pandora. Plaintiffs allege that these Apps “collected personal data from their Android Mobile Phones and shared this data with” Google. (Id. ¶¶ 4, 78-87.) Plaintiffs contend that they were unaware of and did not knowingly consent to collection of this data, which included

Class Members’ home and workplace locations and current whereabouts; several universally unique device identifiers (“UUIDs”) assigned to Plaintiffs’ Android mobile phones; other device-specific data that was useful to Google and third parties for purposes of “device-fingerprinting;” (i.e., the creation of a back-up unique identifier to engage in tracking of a particular device); along with personal information about Plaintiffs such as their gender and age, what functions Plaintiffs performed on Apps, search terms entered, and selections of movies, songs, or restaurants.

(Id. ¶¶ 7-8; see also id. ¶¶ 70-77.) Plaintiffs allege that although Google claimed users could “opt-in” to location tracking, Google actually continually stored their location data, which was transmitted to Google the next time location services were turned on. (Id. ¶ 73.) Plaintiffs also allege that “Google falsely claims that once users opt-in, they will be ‘anonymized’,” because, in truth, “any location data that is sent back to Google location servers is tied and/or traceable to a specific user through the use of UUID’s.” (Id. ¶ 73; see also id. ¶ 30.) Plaintiffs also assert that Google made a number of misrepresentations about the fact that “their personal information would be kept secure,” which led Plaintiffs to believe that Google would not collect and share “their personal information, including their phone use habits and their location.” (Id. ¶¶ 106-115.)

According to Plaintiffs, “this surreptitious use of resources had a real cost to Plaintiffs ... through the consumption and use of battery life, bandwidth, and file storage of their Android Mobile Phones,” and they contend that Google “potentially” exposed them to data overage charges. (Id. ¶¶ 9-14, 98-105.) Plaintiffs also allege that they paid more for their Android Mobile Phones than they would have paid if they had known Google tracked and shared their personal data. (Id. ¶ 13.)
Based on these and other allegations, which the Court shall address as necessary, Plaintiffs bring claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C. section 1030 (the “CFFA Claim”) and violations of California’s Unfair Competition Law, California Business and Professions Code sections 17200, et seq. (the “UCL Claim”).

ANALYSIS

A. Applicable Legal Standards.

1. Federal Rule of Civil Procedure 12(b)(1) (“Rule 12(b)(1)”).

Google moves to dismiss on the basis that Plaintiffs lack standing under Article III of the United States Constitution. The Court evaluates the motion to dismiss for lack of Article III standing pursuant to Rule 12(b)(1). See White v. Lee, 227 F.3d 1214, 1242 (9th Cir. 2000). A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may be “facial or factual.” Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). In this case, Google raises a facial challenge to Plaintiffs’ standing, and, therefore, the Court “must accept as true all material allegations in the complaint, and must construe the complaint in” Plaintiffs’ favor. Chandler v. State Farm Mut. Auto Ins. Co., 598 F.3d 1115, 1121-22 (9th Cir. 2010); see also Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) (“At the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss, [courts] presume that general allegations embrace those specific facts that are necessary to support the claim.”) (internal cite and quotations omitted).

“The jurisdictional question of standing precedes, and does not require, analysis of the merits.” Equity Lifestyle Props., Inc. v. County of San Luis Obispo, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008). Thus, the fact that Plaintiffs may allege facts that, at the pleading stage, satisfy the requirements for Article III standing does not mean these same facts would be sufficient to state a claim. See Doe v. Chao, 540 U.S. 614, 624-25 (2004); In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 n.5 (N.D. Cal. 2011) (quoting Doe, 540 U.S. at 624-25).

2. Federal Rule of Civil Procedure 12(b)(6) (“Rule 12(b)(6)”).

Google also moves to dismiss each of Plaintiffs’ claims pursuant to Rule 12(b)(6). A motion to dismiss is proper under Rule 12(b)(6) where the pleadings fail to state a claim upon
which relief can be granted. In addition, “lack of statutory standing requires dismissal for failure to state a claim[.]” Maya v. Centex Corp., 658 F.3d 1060, 1067 (9th Cir. 2011). On a motion to dismiss under Rule 12(b)(6), the Court construes the allegations in the complaint in the light most favorable to the non-moving party and takes as true all material allegations in the complaint. Sanders v. Kennedy, 794 F.2d 478, 481 (9th Cir. 1986).

Even under the liberal pleading standard of Rule 8(a)(2), “a plaintiff’s obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007) (citing Papasan v. Allain, 478 U.S. 265, 286 (1986)). Rather, a plaintiff must instead allege “enough facts to state a claim to relief that is plausible on its face.” Id. at 570. “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.... When a complaint pleads facts that are merely consistent with a defendant’s liability, it stops short of the line between possibility and plausibility of entitlement to relief.” Ashcroft v. Iqbal, 556 U.S.662, 678 (2009) (quoting Twombly, 550 U.S. at 557) (internal quotation marks omitted).

If a plaintiff’s allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. See, e.g., Reddy v. Litton Indus., Inc., 912 F.2d 291, 296 (9th Cir. 1990); Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc., 911 F.2d 242, 246-47 (9th Cir. 1990).

B. The Court Denies Plaintiffs’ Motion to Strike.

In support of its motion, Google submitted a declaration from Michael H. Rubin, to which it has attached the following exhibits: (1) the Google Privacy Policy dated October 20, 2011; (2) the Android Market Developer Distribution Agreement; (3) and privacy policies and permissions tabs for the Angry Birds, Foursquare, Groupon, Pandora, and Advanced Task Killer Apps. (Docket No. 63.) Plaintiffs move to strike the declaration and the exhibits in their entirety.

Under the “incorporation by reference” doctrine, courts may consider documents that are “referenced extensively in the complaint and [are] accepted by all parties as authentic,” even
if they are not attached to the complaint. *Van Buskirk v. Cable News Network, Inc.*, 284 F.3d 977, 980 (9th Cir. 2002). The Court denies the motion to strike Exhibit A, which is Google’s Privacy Policy. Plaintiffs quote from that document in the SACC, rely on it to support their claims, and have not disputed its authenticity.

Because the Court did not rely on any of the other exhibits to resolve the motion, the Court denies, as moot, the motion to strike these exhibits.

C. **The Court Denies the Motion to Dismiss for Lack of Article III Standing.**

In order to satisfy Article III’s standing requirements, Plaintiffs must show: (1) they suffered an “injury in fact” that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that the injury is fairly traceable to Google’s conduct; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560-61.

Plaintiffs argue that they have Article III standing based on, *inter alia*, the increased rate at which their batteries discharge, which impaired the performance of their phones. The Court previously concluded that these allegations were sufficient to establish Article III standing against Google. *See In re Google*, 2013 WL 1283236, at *5. Google argues that the Court should revisit this ruling. Google may not have manufactured Plaintiffs’ mobile devices, and Plaintiffs may face an uphill battle *proving* this theory of standing. They have alleged sufficient facts to show that they suffered an injury, the injury is fairly traceable to Google’s conduct, and the injury could be redressed by the relief Plaintiffs seek.

Accordingly, the Court denies, in part, Google’s motion to dismiss.3

D. **The Court Grants Google’s Motion to Dismiss the CFAA Claim.**

In their first claim for relief, Plaintiffs assert that Google violated the CFAA. “The

CFAA prohibits a number of different computer crimes, the majority of which involve


3 Because the Court concludes that these facts are sufficient to allege Article III standing, it does not address Plaintiffs alternative theories of standing in this section. The Court shall address those alternative theories, as necessary, in its analysis of the CFAA and UCL claims.
accessing computers without authorization or in excess of authorization, and then taking
specified forbidden actions, ranging from obtaining information to damaging a computer or
computer data.” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1131 (9th Cir. 2009); see also

In order to bring a civil action under the CFAA, Plaintiffs must be able to show a
damage or loss “to 1 or more persons during any 1-year period ... aggregating at least $5,000 in
value.” 18 U.S.C. § 1030 (c)(4)(A)(i)(I), (g). The CFAA defines “damage” as “any impairment
to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. §
1030(e)(8). The CFAA defines “loss” as “any reasonable cost to any victim, including the cost
of responding to an offense, conducting a damage assessment, and restoring the data, program,
system, or information to its condition prior to the offense, and any revenue lost, cost incurred,
or other consequential damages incurred because of interruption of service.” 18 U.S.C. §
1030(e)(11).

Google argues that Plaintiffs’ allegations are insufficient to show the requisite damage
or loss. Plaintiffs rely on the same factual allegations that purport to show Article III standing
to support the “damage” and “loss” elements of the CFAA Claim. (See SACC ¶¶ 137, 147,
149.) For example, Plaintiffs rely on allegations that Google’s conduct diminished the value of
their PII and, as a result, they suffered loss. (SACC ¶ 149.) For the reasons set forth in its
Order granting in part and denying in part Google’s motion to dismiss the First Amended Class
Action Complaint, the Court concludes that these allegations still are insufficient to establish
damage or loss under the CFAA. *See In re Google*, 2013 WL 1283236, at *4, *7-*8.

Plaintiffs also rely on the allegations regarding diminished battery life, and they claim
they have sufficiently alleged damage and loss, because their service was interrupted as a result
of Google’s conduct. Plaintiffs contend these allegations distinguish this case from *In re
iPhone App. Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012) (“*iPhone App. Litig. II*”). In that
case, the court found that plaintiffs had not included facts to suggest the defendant’s conduct
“impaired” their devices or interrupted service and, thus, failed to show damage or loss under
the CFAA. *See id.*, 844 F. Supp. 2d at 1067. Here, Plaintiffs do allege that Google’s conduct
interrupted their service. That fact might be sufficient to satisfy the definition of “damage” set forth in 18 U.S.C. section 1030(e)(8). However, in order to pursue a civil action under the CFAA, Plaintiffs also must show *economic damage or loss* in the amount $5,000. 18 U.S.C. § 1030 (c)(4)(A)(i)(I). Plaintiffs allege that a new battery could cost $70.00. However, none of the Plaintiffs allege that they did purchase new batteries because of Google’s conduct. (*See, e.g.,* SACC ¶¶ 98-102.) The Court concludes that the allegations regarding diminished battery life still are insufficient to allege that the economic damage or loss - even if aggregated - would reach the $5,000 threshold required by the CFAA.

Finally, Plaintiffs rely on allegations that they paid for their data plans, and that Google “used or allowed the use of a finite amount of” their data plans. Again, none of the named Plaintiffs alleged that they incurred *any* overage charges. Rather, they only allege that they were “potentially” exposed to overage charges.⁴ (SACC ¶¶ 103-105.) The Court concludes that the allegations regarding “loss” based on “Data Plan Utilization” are insufficient to allege that the economic damage or loss - even if aggregated - would reach the $5,000 threshold required by the CFAA. *See, e.g.,* iPhone App. Litig. II, 844 F. Supp. 2d at 1067.

Accordingly, the Court grants Google’s motion to dismiss the CFAA Claim. This is Plaintiffs’ third iteration of the complaint, and the Court concludes that any further attempts to amend this claim would be futile.

E. The Court Grants, in Part, and Denies, in Part, Google’s Motion to Dismiss the UCL Claim.

Plaintiff’s second claim for relief is a claim under the UCL, which prohibits “three varieties of unfair competition: practices which are unlawful, unfair or fraudulent.” *Daugherty v. American Honda Motor Co.*, 144 Cal. App. 4th 824, 837 (2006); *see also* *Albillo v. Intermodal Container Services, Inc.*, 114 Cal. App. 4th 190, 206 (2003) (to state a UCL claim, a “plaintiff must establish that the practice is either unlawful (i.e., is forbidden by law), unfair

⁴ That fact distinguishes this case from the facts in the related case *Yunker v. Pandora Media*, 13-CV-3113-JSW.
(i.e., harm to victim outweighs any benefit) or fraudulent (i.e., is likely to deceive members of the public”).

The UCL also “requires that a plaintiff have ‘lost money or property’ to have standing to sue. The plain import of this is that a plaintiff now must demonstrate some form of economic injury.” *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011); *see also* Cal. Bus. & Prof. Code § 17204. “California courts have distinguished the UCL standing requirement as more stringent than the federal Article III standing requirement,” because of the requirement that a UCL plaintiff have lost money or property. *Pirozzi v. Apple, Inc.*, – F. Supp. 2d –, 2013 WL 4029067, at *5 (N.D. Cal. Aug. 5, 2013). However, there are many ways a plaintiff may establish economic injury to show standing under the UCL, including “surrender[ing] in a transaction more, or acquir[ing] in a transaction less, than he or she otherwise would have.” *Kwikset*, 51 Cal. 4th at 323; *see also id.* at 325 (allegations of “personal, individualized loss of money or property in any nontrivial amount” is sufficient to allege injury in fact under UCL).

Google moves to dismiss this claim for lack of statutory standing, and it also argues that Plaintiffs fail to allege facts that show Google violated the UCL.

1. **Plaintiffs Have Statutory Standing to Pursue the UCL Claim.**

   Plaintiffs contend they have standing under the UCL based on the allegations that they “paid more than they otherwise would have for their phones, lost available data on their data plans, and suffered diminished battery life.” (SACC ¶ 156.) For the reasons set forth in its previous Order, the Court concludes that Plaintiffs have alleged sufficient facts to show standing based on the diminished battery life. *See In re Google*, 2013 WL 1283236, at *8; *see also Goodman v. HTC America, Inc.*, 2012 WL 2412070, at *12 (W.D. Wash. June 26, 2012).

   Accordingly, the Court denies, in part, Google’s motion to dismiss.

2. **Plaintiffs Fail to State a Claim Under the Unlawful Prong.**

   To state a claim based on the unlawful prong, Plaintiffs must allege that the Google Defendants’ practices are “forbidden by law, be it civil, criminal, federal, state, or municipal, statutory, regulatory, or court made.” *Saunders v. Superior Court*, 27 Cal. App. 4th 832, 838-39 (1994). “[A] violation of another law is a predicate for stating a cause of action” under the

Plaintiffs fail to allege facts showing a violation of the CFAA, and they do not identify any other statutes that could support a claim under the unlawful prong. Plaintiffs also have not provided the Court with any authority that the alleged violations of the settlement described in paragraph 20 of the SACC could support this claim.

Accordingly, Plaintiffs fail to state a claim under the unlawful prong, and the Court grants, in part, Google’s motion to dismiss.

3. **Plaintiffs State a Claim Under the Unfair Prong.**

Google also argues that Plaintiffs fail to state a claim under the unfair prong. Unfair simply means any practice whose harm to the victim outweighs any benefits. *Olsen v. Breeze, Inc.*, 48 Cal. App. 4th 608, 618 (1996). “The court must weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *Gafcon, Inc. v. Ponsor & Assocs.*, 98 Cal. App. 4th 1388, 1425 n.15 (2002). In *iPhone App. Litig. II*, the court found that allegations regarding collection and dissemination of personal information, which are similar to Plaintiffs’ allegations, were sufficient to state a claim under the unfair prong. *iPhone App. Litig. II*, 844 F. Supp. 2d at 1073.

In its previous order, the Court found that Plaintiffs had alleged UCL standing for their claims against Google. It also stated that Plaintiffs could state a claim under this prong, if they were able to allege standing. Because Google is the only remaining defendant, Plaintiffs state a claim under the unfair prong.

Accordingly, the Court denies, in part, Google’s motion to dismiss.

4. **Plaintiffs State a Claim Under the Fraudulent Prong.**

Plaintiffs also assert that the Google’s conduct violates the fraudulent prong of the UCL. (See SACC ¶¶ 162-167.) To state a cause of action under the fraudulent prong of Section 17200, it is necessary only to show members of the public are likely to be deceived; allegations that the fraudulent deception was “actually false, known to be false by the perpetrator and
reasonably relied upon by a victim who incurs damages” are not necessary. *In re Tobacco II Cases*, 46 Cal. 4th 298, 312 (2009).

Google argues that, although Plaintiffs have alleged the purportedly false statements with specificity, they still fail to allege facts showing why the statements were false. It also argues that Plaintiffs’ allegations are directly contradicted by the terms of its Privacy Policy. The Court finds that Plaintiffs’ allegations are similar to the allegations in *iPhone App. Litig. II*. Specifically, Plaintiffs contend that Google’s representations that users can opt-in to location monitoring is false, because Google continues to track and store information even when the location services feature is turned off. *Cf. iPhone App. Litig. II*, 844 F. Supp. 2d at 1074.

In addition, the plaintiffs allege that contrary to the representations in Google’s privacy policy, Google designed the AOS “to enable and promote the taking of Plaintiffs ... personal information so as to further monetize, for [Google’s] benefit, the advertising potential of AOS-based devices and to advance Google’s revenue model in the wireless/mobile marketplace.” (SACC ¶ 3; *see also id.* ¶ 4 (alleging that Google collected and transmitted PII “for purposes wholly unrelated to the use and functionality of” an Android mobile device or App). These allegations are similar to the allegations made by the “iDevice Class” in *iPhone App. Litig. II*. See 844 F. Supp. 2d at 1074.

The Court concludes that these allegations, in combination with the allegations that Plaintiffs relied on these statements and paid more for their mobile devices than they otherwise would have are sufficient to *allege* a claim under the fraudulent prong.

Accordingly, the Court denies, in part, Google’s motion to dismiss.

4. **The Court denies Google’s motion to dismiss the claim for restitution.**

Google also moves to dismiss Plaintiffs’ claim for restitution under the UCL on the basis that, because Plaintiffs did not pay any money to Google, they are asking for “non-restitutionary disgorgement,” which is not an available remedy under the UCL. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1145 (2003). In *Ferrington v. McAfee*, the district court rejected a similar argument, and stated that the “distinction California courts have drawn between restitutionary disgorgement and non-restitutionary disgorgement does not turn
on whether Plaintiffs paid money directly to the defendant. It turns, rather, on whether the
profits sought to be disgorged would merely ‘restore the status quo by returning to the plaintiff
funds in which she has an ownership interest’ or would achieve something broader.” Id., 2010
F.3d 977, 996 (9th Cir. 2006)).

Although Plaintiffs do not allege facts that show they paid money directly to Google, the
Court cannot conclude that Plaintiffs might not be able to show an ownership interest in at least
some of Google’s profits. Cf. Colgan v. Leatherman Tool Group, Inc., 135 Cal. App. 4th 663,
699 (2006) (a plaintiff can seek money or property as restitution where such “money or property
identified as belonging in good conscience to the plaintiff could clearly be traced to particular
funds or property in the defendant’s possession”) (citation omitted).

Accordingly, the Court denies, in part, Google’s motion to dismiss. However, the Court
shall not preclude Google from renewing this argument as this case progresses.

5. The Court denies the motion to dismiss the non-California plaintiffs.

Google also moves to dismiss the UCL claims brought by Mr. Lawrence, Ms. Hillman-
Seidner, Ms. Smith, Mr. Hall, and Ms. Urias, on the basis that they are not California residents.
In support of this argument, Google relies on Mazza v. American Honda Motor Co., 666 F.3d
In Mazza, the defendant was headquartered in California, and the plaintiffs alleged that the
allegedly fraudulent misrepresentations emanated from California. However, the transactions
that purportedly injured class members took place outside California. Mazza, 660 F.3d at 590.
The Ninth Circuit reversed the district court’s decision to certify a nationwide class for alleged
violations of the UCL, and it held that “[u]nder the facts and circumstances of this case, we hold
that each class member’s consumer protection claim should be governed by the consumer
protection laws of the jurisdiction in which the transaction took place.” Id. at 594.

Plaintiffs argue that the Mazza argument is premature and should be addressed at the
class certification phase. In the Frezza case, the district court rejected a similar argument, and
found that the choice-of-law principle announced in Mazza “applies generally and is instructive
even when addressing a motion to dismiss.” Frezza, 2013 WL 1736788, at *6; see also id., at *5 (“The factual analogy makes Mazza’s application of the choice-of-law rule to the facts of this case, not only relevant but controlling.”). However, in both Mazza and Frezza, the courts engaged in a choice-of-law analysis to determine which state’s law should apply.

Google raised this argument in a footnote, and it presents no argument as to why Texas and Alabama law would conflict with California law. Accordingly, the Court concludes that Google has not met its burden to show the claims of non-California plaintiffs should be dismissed. This ruling is without prejudice to Google renewing this argument in a subsequent motion.

**CONCLUSION**

For the foregoing reasons, the Court grants, in part, and denies, in part, Google’s motion to dismiss. The Court ORDERS the parties to appear for a case management conference on April 18, 2014 at 11:00 a.m., in Courtroom 5, Second Floor, 1301 Clay Street, Oakland, California. The parties’ joint case management statement shall be due by no later than April 11, 2014.

**IT IS SO ORDERED.**

Dated: March 10, 2014

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE
NOT FOR PUBLICATION

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

TROY YUNKER, EDGAR DURAN, ROBERT HODSON, and RALPH PETROSI N, et al.,

Plaintiffs,

v.

PANDORA MEDIA, INC.,

Defendant.

No. 11-CV-03113 JSW

ORDER GRANTING IN PART AND DENYING IN PART PANDORA MEDIA, INC.’S MOTION TO DISMISS SECOND AMENDED COMPLAINT AND SETTING CASE MANAGEMENT CONFERENCE

(Docket No. 83)

Now before the Court for consideration is motion to dismiss filed by Defendant Pandora Media, Inc. (“Pandora”). The Court has considered the parties’ papers, relevant legal authority, the record in this case, and it HEREBY GRANTS, IN PART, AND DENIES, IN PART, the motion to dismiss.¹

BACKGROUND

“This action challenges Pandora’s practice of collecting the personal information of its users and then disseminating it to third-party advertising libraries.” (Docket No. 79, Second Amended Class Action Complaint (“SACC”) ¶ 1.)² Plaintiffs, citizens of Illinois, Troy Yunker

¹ Plaintiffs have not complied with Northern District Local Rule 3-4(c)(2), which requires that footnotes be in 12 point font. The Court HEREBY places all parties on notice that if any party fails to comply with this rule in the future, the Court shall strike the offending brief without further notice to that party.

(“Mr. Yunker”), Edgar Duran (“Mr. Duran”), Robert Hodson (“Mr. Hodson”), and Ralph Petrosino (“Mr. Petrosino”) (collectively “Plaintiffs”) downloaded and used the Pandora App on their mobile devices.  

Mr. Petrosino, Mr. Duran, and Mr. Hodson also paid recurring monthly fees for Pandora’s premium service, Pandora One (hereinafter the “Pandora One Plaintiffs”).  

Plaintiffs allege that when they downloaded and registered to use the Pandora App, Pandora collected “certain personally identifiable information (‘PII’) ... including” age, gender, location and the universally unique device identifier (“UUID”) for a user’s mobile device.

Pandora’s Privacy Policy provides, in part, that it may:

use and share non-personally identifiable information, such as general demographic or location information, or information about the computer or device from which you access [the Pandora App]. Additionally, we may de-identify personally identifiable information and share it in a de-identified or aggregated form with third parties, advertisers and/or business partners in order to analyze [Pandora] usage, improve the Pandora Services and your listener experience, or for other similar purposes. The use and disclosure of such information is not subject to any restrictions under the Privacy Policy.

In return for Pandora’s promises to share PII only in a “de-identified or aggregated form” and “only for purposes of using the Pandora App itself,” Plaintiffs permitted “Pandora to utilize exclusively de-identified PII and non-personally identifiable information.”

Plaintiffs allege that “Pandora did not explain - and consumers were unaware - that the information was not used for purposes of the Pandora application itself, but rather for the transmission and commercialization of the information by way of third-party advertisers.”

3 Pandora attached a copy of its Privacy Policy, in effect as of January 30, 2012, to a request for judicial notice.  

4 None of Plaintiffs’ claims are premised on allegations that Pandora failed to live up to its promise that it would provide Plaintiffs with music streaming services.
Plaintiffs allege that PII is valuable private property, and they did not grant Pandora consent to distribute their PII to third-parties. (Id. ¶¶ 44-45, 48-50.) Plaintiffs also allege that Pandora installed “certain code components” on their mobile devices, which consumed portions of the ‘cache’ and/or gigabytes of memory.” (Id. ¶ 51.) Plaintiffs allege that they paid money for the exclusive use of that memory, and they allege that mobile device manufacturers charge their customers a premium to purchase extra memory on the devices. (Id. ¶ 52.) According to Plaintiffs, because the Pandora App used more bandwidth and data than was necessary to operate, absent the collection of their PII, they paid monthly fees for data plans on their mobile devices, incurred additional fees when they exceeded their monthly allotments, and had less available data each month. (Id. ¶¶ 43-59.)

Plaintiffs allege that they would not have downloaded the Pandora App and provided Pandora with their PII, had they known how Pandora actually treated and used their PII. In addition, the Pandora One Plaintiffs allege that they would not have paid for Pandora One had they known how Pandora actually treated and used their PII. (Id. ¶¶ 7-10, 60-63.)

Based on these, and other allegations, Plaintiffs assert claims for violations of California Business and Profession Code section 17200, et seq., (the “UCL Claim”), breach of contract, and violations of Article I, Section I of the California Constitution (the “Right to Privacy Claim”).

ANALYSIS

A. Applicable Legal Standards.

1. Federal Rule of Civil Procedure 12(b)(1) (“Rule 12(b)(1)”).

Pandora moves to dismiss Plaintiffs’ first and second claims for relief on the basis that Plaintiffs lack standing under Article III of the United States Constitution. The Court evaluates the motion to dismiss for lack of Article III standing pursuant to Rule 12(b)(1). See White v. Lee, 227 F.3d 1214, 1242 (9th Cir. 2000). A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may be “facial or factual.” Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). Pandora raises a facial challenge to Plaintiffs’ standing. Therefore, the Court “must accept as true all material allegations in the complaint, and must
construe the complaint in" Plaintiffs’ favor. Chandler v. State Farm Mut. Auto Ins. Co., 598 F.3d 1115, 1121-22 (9th Cir. 2010); see also Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) (“At the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion dismiss, [courts] presume that general allegations embrace those specific facts that are necessary to support the claim.”) (internal cite and quotations omitted).

“The jurisdictional question of standing precedes, and does not require, analysis of the merits.” Equity Lifestyle Props., Inc. v. County of San Luis Obispo, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008). Thus, the fact that Plaintiffs may allege facts that, at the pleading stage, satisfy the requirements for Article III standing does not mean these same facts would be sufficient to state a claim. See Doe v. Chao, 540 U.S. 614, 624-25 (2004); In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 n.5 (N.D. Cal. 2011) (quoting Doe, 540 U.S. at 624-25).

2. Federal Rule of Civil Procedure 12(b)(6) ("Rule 12(b)(6)").

Pandora also moves to dismiss each of Plaintiffs’ claims pursuant to Rule 12(b)(6). A motion to dismiss is proper under Rule 12(b)(6) where the pleadings fail to state a claim upon which relief can be granted. A motion to dismiss for “lack of statutory standing requires dismissal for failure to state a claim[.]” Maya v. Centex Corp., 658 F.3d 1060, 1067 (9th Cir. 2011). The Court construes the allegations in the complaint in the light most favorable to the non-moving party, and it takes as true all material allegations in the complaint. Sanders v. Kennedy, 794 F.2d 478, 481 (9th Cir. 1986).

Even under the liberal pleading standard of Rule 8(a)(2), “a plaintiff’s obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007) (citing Papasan v. Allain, 478 U.S. 265, 286 (1986)). Instead, a plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” Id. at 570. “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully. ... When a complaint pleads facts that are merely consistent with a defendant’s liability, it stops short of the line

If a plaintiff’s allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. *See, e.g., Reddy v. Litton Indus., Inc.*, 912 F.2d 291, 296 (9th Cir. 1990); *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246-47 (9th Cir. 1990).

**B. The Court Denies the Motion to Dismiss for Lack of Article III Standing.**

In order to satisfy Article III’s standing requirements, Plaintiffs must show: (1) they suffered an “injury in fact” that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that the injury is fairly traceable to Pandora’s conduct; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560-61. Plaintiffs argue, *inter alia*, that they have standing because Pandora’s conduct decreased the amount of memory space on their mobile devices.

Courts have found that “[d]imunition in the performance of an electronic device may constitute an injury in fact, but a plaintiff must ‘allege facts showing that this is true.’” *Goodman v. HTC America, Inc.*, 2012 WL 2412070, at *6 (W.D. Wash. June 26, 2012) (quoting *LaCourt v. Specific Media*, 2011 WL 1661532, at *5 (C.D. Cal. Apr. 28, 2011) (emphasis added); *see also In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1054-56 (N.D. Cal. 2012) ("*iPhone App. Litig. II*“). For example, in *iPhone App. Litig. II*, the plaintiffs alleged that they paid for the “exclusive use” of the memory on their phones. The court concluded that allegations regarding diminished storage, battery life, and bandwidth were sufficient to allege actual injury. *Id.* at 1054.

Although the Court previously concluded that Mr. Yunker had not alleged sufficient facts to premise Article III standing on this theory, Plaintiffs’ allegations in the SACC are
similar to the allegations in *iPhone App. Litig. II*.5 Plaintiffs allege that the Pandora App “consumed more bandwidth than was necessary absent the collection of Plaintiff’s [sic] PII,” and that “more data was consumed by the [Pandora] App than was necessary[.]” (SACC ¶ 55, 57.) According to Plaintiffs, as a result, they had less available data each month, and they allege they incurred additional fees when their monthly allotments were exceeded. (Id. ¶¶ 55-58.) Plaintiffs also allege that “the presence and surreptitious activities of the third-party advertising libraries in the Pandora App include certain code components that ... consumed portions of the ‘cache’ and/or gigabytes of memory” available to them. (Id. ¶ 51.) Plaintiffs further allege that Pandora consumed the memory available to Plaintiffs for its “own purposes,” and that this “constitutes a taking of an asset of economic value, paid for by Plaintiffs.” (Id. ¶ 54.) In addition, the Pandora One Plaintiffs allege they paid monthly fees for the premium service and allege they would not have purchased that service had they known how Pandora was using their PII. Plaintiffs may face an uphill battle proving that they have standing Article III standing6, but they set forth sufficient facts to allege Article III standing.

Accordingly, the Court denies, in part, Pandora’s motion to dismiss.

C. The Court Denies Pandora’s Motion to Dismiss the UCL Claim.

1. Plaintiffs Have Statutory Standing to Pursue the UCL Claim.

In their first claim for relief, Plaintiffs allege Pandora violated the UCL. Pandora argues that Plaintiffs lack statutory standing to pursue this claim. The UCL “requires that a plaintiff have ‘lost money or property’ to have standing to sue. The plain import of this is that a plaintiff now must demonstrate some form of economic injury.” *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011); see also Cal. Bus. & Prof. Code § 17204. “California courts have

5 *See, e.g., In re iPhone App. Litig.*, 11-md-2250-LHK, First Amended Consolidated Complaint (“*iPhone App. Lit. FAC*”), ¶¶ 63.b, 72.d, 198.) Pandora requests that the Court take judicial notice of the First Amended Complaint filed in *In re iPhone App Litig.*, and it has attached the complaint as Exhibit A to the Declaration of Tyler Newby. (Docket No. 89, Reply Request for Judicial Notice; Docket No. 90, Declaration of Tyler Newby.) Plaintiffs have not objected to that request. Because the Court can take judicial notice of the existence of court records, and because the Court is not reviewing the complaint for the truth of the facts alleged therein, the Court GRANTS the request for judicial notice.

distinguished the UCL standing requirement as more stringent than the federal Article III standing requirement,” because of the requirement that a UCL plaintiff have lost money or property. *Pirozzi v. Apple, Inc.*, – F. Supp. 2d –, 2013 WL 4029067, at *5 (N.D. Cal. Aug. 5, 2013). However, there are many ways a plaintiff may establish economic injury to show standing under the UCL, including “surrender[ing] in a transaction more, or acquire[ing] in a transaction less, than he or she otherwise would have.” *Kwikset*, 51 Cal. 4th at 323; *see also id.* at 325 (allegations of “personal, individualized loss of money or property in any nontrivial amount” is sufficient to allege injury in fact under UCL).

As set forth above, Plaintiffs allege that they paid for the exclusive use of the memory and for data plans on their devices, *and* incurred additional fees when monthly allotments were exceeded. The Plaintiffs also allege that this economic injury was caused by the fact that the Pandora App used more data than was necessary when it collected and shared their PII with third-parties. Plaintiffs have *alleged* sufficient facts to show they have standing to pursue the UCL claim.

Accordingly, the Court denies, in part, Pandora’s motion to dismiss.

2. Plaintiffs State a Claim Under the Unfair Prong of the UCL.

Under the UCL, “there are three varieties of unfair competition: practices which are unlawful, unfair or fraudulent.” *Daugherty v. American Honda Motor Co.*, 144 Cal. App. 4th 824, 837 (2006); *see also Albillo v. Intermodal Container Services, Inc.*, 114 Cal. App. 4th 190, 206 (2003) (to state a UCL claim, a “plaintiff must establish that the practice is either unlawful (i.e., is forbidden by law), unfair (i.e., harm to victim outweighs any benefit) or fraudulent (i.e., is likely to deceive members of the public)”). Plaintiffs’ UCL claim appears to be premised solely on the “unfair” prong. (*See SACC ¶ 80.*)

Pandora argues that Plaintiffs fail to state a claim under the unfair prong. The Court addressed this issue in its Order resolving Pandora’s motion to dismiss the First Amended Complaint and concluded that, if Mr. Yunker could allege facts to show he had standing, he had alleged sufficient facts to state a claim under the unfair prong. *Yunker*, 2013 WL 1282980, at
*12. Because Plaintiffs allege sufficient facts to show they have statutory standing, they have now stated a claim under the unfair prong.

Accordingly, the Court denies, in part, Pandora’s motion to dismiss

**D. The Court Denies the Motion to Dismiss the Breach of Contract Claim**

In their second claim for relief, Plaintiffs allege that Pandora breached the terms of its Privacy Policy. In order to state a claim for breach of contract, Plaintiffs must allege: (1) the existence of a contract; (2) they performed under the contract; (3) Pandora breached the contract; (4) and they suffered appreciable and actual damage as a result of Pandora’s breach.


Pandora argues that the Privacy Policy is not a contract. Plaintiffs allege that they transmitted PII, which has value to Pandora, in exchange for use of the Pandora App and a promise that Pandora would use that information in accordance with the terms of its Privacy Policy. Based on these allegations, and at this stage of the proceedings, the Court concludes that Plaintiffs sufficiently allege a contract existed. In addition, and contrary to Pandora’s argument, Plaintiffs incorporate the “device resource utilization allegations,” in the breach of contract claim. (See SACC ¶ 87 (incorporating by reference paragraphs 1-75).) Thus, Plaintiffs allege that because Pandora used and transmitted PII in a manner that did not comport with the terms of the Privacy Policy, they incurred overage charges on their data and memory plans, *i.e.* they suffered damage as a result of the alleged breach. Once again, although Plaintiffs may face an uphill battle proving this claim, they have stated a claim.

Accordingly, the Court denied, in part, Pandora’s motion to dismiss.

**E. The Court Dismisses the Right to Privacy Claim With Prejudice.**

In their third claim for relief, Plaintiffs allege that Pandora violated their right to privacy under the California Constitution. In order to state a Right to Privacy claim, Plaintiffs must allege facts showing: (1) a specific, legally protected privacy interest; (2) a reasonable
expectation of privacy; and (3) conduct that is “sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.” *Hill v. Nat’l Collegiate Athletic Ass’n*, 7 Cal. 4th 1, 35-37 (1994); *see also iPhone App Litig. II*, 844 F. Supp. 2d at 1063. This case raises the issue of “informational privacy,” *i.e.* the alleged “dissemination or misuse of sensitive and confidential information....” *Hill*, 7 Cal. 4th at 35.

The Court has considered the new allegations in the SACC. For the reasons set forth in its previous order, the Court concludes that the Plaintiffs still fail to allege facts that satisfy the third element of this claim. *See Yunker*, 2013 WL 1282980, at *14-*15. Because this is the third iteration of Plaintiffs’ complaint, the Court concludes that any further amendments would be futile.

Accordingly, the Court grants, in part, Pandora’s motion to dismiss, and it dismisses the Right to Privacy Claim, without leave to amend.

**CONCLUSION**

For the foregoing reasons, the Court GRANTS, IN PART, AND DENIES, IN PART, Pandora’s motion to dismiss. The parties are HEREBY ORDERED to appear for a case management conference on April 18, 2014 at 11:00 a.m. in Courtroom 5, Second Floor, 1301 Clay Street, Oakland, California. The parties shall submit a joint case management statement by no later than April 11, 2014.

**IT IS SO ORDERED.**

Dated: March 10, 2014

[JEFFREY S. WHITE]
UNITED STATES DISTRICT JUDGE
I. Introduction

Surely, one of the unwelcome consequences of the digital age are unsolicited messages, telephone calls, and emails. However, this phenomenon is not new. Unwelcome circumstances have faced characters in literature and opera for centuries. Victims of circumstance are often portrayed by Shakespeare – Hamlet, Othello, Shylock; and in opera, Verdi’s Don Carlos, who without fault, loses his fiancée, Elisabeth of Valois, to his own father, King Phillip of Spain, who marries Elisabeth to ensure peace with France.

In this case, Plaintiff Bill Dominguez is also a victim of circumstance. Plaintiff purchased a cellular telephone and was assigned a phone number. The previous owner of the telephone number had enrolled the number in a text message system of Defendant, Yahoo!, Inc. (“Yahoo”). Plaintiff, on behalf of himself and other similarly situated consumers, initiated this class action lawsuit against Defendant, Yahoo!, Inc. (“Yahoo”) to challenge Yahoo’s practice of sending unsolicited text messages to cellular telephone numbers owned by individuals who never consented to receive such text messages. He seeks statutory damages, treble damages, costs, fees, a declaratory judgment, and an injunction on behalf of his claim. Is Yahoo responsible for Plaintiff’s damages?
II. Procedural History

Plaintiff filed his Complaint against Yahoo on April 10, 2013. ECF 1. Plaintiff alleges that Yahoo violated the Telephone Consumer Protection Act (“TCPA”), enacted by Congress in 1991. This Court has jurisdiction pursuant to 28 U.S.C. § 1331, which provides that “[t]he district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.”


This Court held oral argument on the Motion for Summary Judgment and related briefing on March 11, 2014.

III. The Parties’ Contentions

A. Yahoo’s Motion for Summary Judgment

Yahoo does not dispute that Plaintiff received text messages solely because a Yahoo subscriber, who previously used the same mobile phone number that was subsequently assigned
to Plaintiff, affirmatively signed up to receive text messages each time he received an email in his Yahoo email inbox. Yahoo argues that the TCPA only prohibits unsolicited automated telemarketing and bulk communications sent via an Automatic Telephone Dialing System (“ATDS”), which means a system that has the capacity to store or produce telephone numbers to be called using a random or sequential number generator, and dials those numbers. 47 U.S.C. § 227(b)(3).

Yahoo contends that its system is not an ATDS because the system lacks the capacity to store or produce telephone numbers to be called, using a random or sequential number generator.

Yahoo also disputes that the messages it sent fall within the purview of the TCPA, which was intended to regulate the sending of unsolicited advertisements or bulk communication, not messages forwarded at the request of a user. Yahoo asks this court to conclude that the TCPA does not apply to the present facts because the notifications were specifically requested, and sent to the mobile phone number provided by a Yahoo email account user at the user’s request and only once the user had received an email.

**B. Plaintiff’s Opposition to Motion for Summary Judgment**

To begin, Plaintiff points out that Yahoo does not dispute that Plaintiff himself never solicited the text messages that he received from Yahoo, and he argues that consent must be given from the current subscriber, not a previous owner of the telephone number.

Plaintiff then disputes Yahoo’s contention that its system is not an ATDS. Plaintiff argues that courts must look to the system’s capacities, not the way in which it is actually used, and argues that the capacities of Yahoo’s system fall within the statutory definition. ECF 39 (Pl.’s Opp’n to Def.’s Mot. for Summ. J.) at 13 (citing Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 951 (9th Cir. 2006)).
In support of his position, Plaintiff relies on the Declaration of Randall Snyder, a
purported expert in the fields of wireline and wireless telecommunications networking
technology,¹ and the deposition testimony of Yahoo’s corporate representative, Mr.
Gopalkrishna. ECF 39 (Pl.’s Opp’n to Def.’s Mot. for Summ. J.) (citing Snyder Decl.;

C. Yahoo’s Reply

In Reply, Yahoo contends that Mr. Snyder’s opinion does not create a material factual
dispute because he merely states a legal conclusion that the Email SMS Service is an ATDS, and
that conclusion is based on an illogical interpretation of the statute. Yahoo specifically takes
issue with Mr. Snyder’s interpretation of the term “sequential” (Mr. Snyder defines the term to
mean that messages are sent “one at a time” as opposed to all at once), his misunderstanding that
the statute concerns sequential sending of text messages as opposed to the generation of
telephone numbers, and his acknowledgement, in deposition testimony, that, based on his
interpretation of the statutory language, every text message system currently in existence sends
messages sequentially. Moreover, Yahoo argues, Mr. Snyder has not reviewed any of the
messages sent via the Email SMS² Service or the software or programming used by the Email
SMS Service, but only reviewed the written specifications that Mr. Snyder admitted may differ
from the way in which the system actually works.

¹ Mr. Snyder has been retained as a testifying or consulting expert in 65 cases regarding cellular technology,
including 41 cases regarding text messaging technology, and 33 cases regarding the TCPA and associated
regulations. Snyder Decl. ¶ 4. Plaintiff also submitted to this Court a Notice containing Supplemental Authority in
support of his Opposition to Defendant’s Motion to Dismiss, in which the Southern District of California relied on a
declaration offered by Mr. Snyder regarding Yahoo’s text messaging service. ECF 46 (containing Memorandum of
Mr. Snyder did admit in his deposition that the technology at issue in Sherman is different from that at issue in the
present litigation. Declaration of Justin A. Barton in Support of Def.’s Reply to Resp. to Mot. for Summ. J., Ex. 1
(Snyder Dep.) at 136:17-137:4.
² SMS is an acronym for “short message service,” or what is more commonly referred to as text messaging.
Yahoo also argues that this Court should not credit Mr. Snyder’s opinions because they are driven by his own personal interest, since his wife is the named plaintiff in a class action lawsuit related to his son’s receipt of a single, unsolicited text message from a recycled phone number. ECF 47 (Def.’s Reply in Supp. of Mot. for Summ. J.) at 12 (citing Snyder Tr. 45:12-50:15). Yahoo contends that his wife’s class action would be directly undermined if this Court rejects Mr. Snyder’s conclusions here. Lastly, Yahoo argues that Mr. Snyder lacks credibility because he is personally interested in fighting against “spam” text messages and earns 80-90% of his income from testifying in TCPA cases. Id. at 13 (citing Snyder Tr. 52:14-53:17, 75:4-8, 83:20-84:5).

D. Plaintiff’s Sur Reply

Plaintiff submitted a short Sur Reply arguing that the testimony from Yahoo’s own witness shows that the Email SMS Service is an ATDS, responding to Yahoo’s arguments regarding the definition of the term “sequential,” and defending the validity of the Snyder Declaration.

IV. Legal Standard

Summary judgment is appropriate “if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c). An issue is “genuine” if the evidence is such that a reasonable jury could return a verdict for the non-moving party. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). A factual dispute is “material” if it might affect the outcome of the case under governing law. Id.

A party seeking summary judgment always bears the initial responsibility for informing the district court of the basis for its motion and identifying those portions of the record that it believes demonstrate the absence of a genuine issue of material fact. Celotex Corp. v. Catrett,
477 U.S. 317, 322 (1986). Where the non-moving party bears the burden of proof on a particular issue at trial, the moving party’s initial burden can be met simply by “pointing out to the district court that there is an absence of evidence to support the non-moving party’s case.” Id. at 325. After the moving party has met its initial burden, the adverse party’s response must, “by affidavits or as otherwise provided in this rule [ ] set out specific facts showing a genuine issue for trial.” Fed. R. Civ. P. 56(e). Summary judgment is appropriate if the non-moving party fails to rebut by making a factual showing “sufficient to establish the existence of an element essential to that party’s case, and on which that party will bear the burden of proof at trial.” Celotex, 477 U.S. at 322. Under Rule 56, the Court must view the evidence presented on the motion in the light most favorable to the opposing party. Anderson, 477 U.S. at 255.

VI. Discussion

The TCPA prohibits any person from making:

any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any [ATDS] . . .

(iii) to any telephone number assigned to a . . . cellular telephone service . . . or any service for which the called party is charged for the call . . . .


---

3 Yahoo “assume[s] without conceding for purposes of this motion that a text message constitutes a ‘call’ within the meaning of the TCPA.” ECF 14 (Def.’s Mot. for Summ. J.) at 6. Federal courts have made clear that the TCPA applies to text messages as well as voice calls. Gager v. Dell Fin. Servs., LLC, 727 F.3d 265, 268 (3d Cir. 2013) (citing In the Matter of Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 27 F.C.C. Rcd. 15391 (2012) and Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 954 (9th Cir. 2009)).
The parties disputes relate to two issues: first, whether Yahoo’s Email SMS Service meets the statute’s definition of an “ATDS,” and second, whether the messages sent to Plaintiff constitute advertisements such that they are covered by the statute.

1. ATDS

The statute defines an ATDS as “equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.” Id. § 227(a)(1).

The Ninth Circuit clarified that when a court evaluates the issue of whether equipment is an ATDS, “the statute’s clear language mandates that the focus must be on whether the equipment has the capacity ‘to store or produce telephone numbers to be called, using a random or sequential number generator.’” Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 951 (2009) (emphasis in original). The court continued: “[A] system need not actually store, produce, or call randomly or sequentially generated telephone numbers, it need only have the capacity to do so.” Id.

From the mid-2000s until June 2011, Yahoo offered its email account holders the option to sign up for a program that allowed customers to register a mobile telephone number to which Yahoo would send an SMS or text message to the customer when he or she received an email.

ECF 14 at 2. The parties largely agree on the basic functions of the system Yahoo used to send these text message, or what the parties refer to as the Email SMS Service. That system automatically converted email messages into a truncated format, accessed the appropriate user’s telephone number from a stored list, and automatically sent the text message to the customer’s
mobile device. Id. at 3; Gopalkrishna Dep. 52:8-15, 72:20-73:13. Mr. Ajay Gopalkrishna is employed by Yahoo as the Senior Product Manager for Yahoo! Mail Anti-Spam and Delivery, through which he has personal knowledge and/or information regarding Yahoo’s Email SMS System. Gopalkrishna Decl. ¶ 1. The Email SMS Service also included a queuing program that would order and store outgoing text messages. Gopalkrishna Dep. 98:2-7.

The parties do dispute, however, whether the system’s capabilities fall within the statutory definition of an ATDS. Yahoo argues that Plaintiff has not shown that its system could or did have the capacity to randomly or sequentially generate telephone numbers. Further, Yahoo offers the Declaration of Ajay Gopalkrishna as evidence that its system did not in fact have that capacity. ECF 14-1 (“Gopalkrishna Decl.”). In his Declaration, Mr. Gopalkrishna asserts that “[t]he servers and systems affiliated with the Email SMS Service did not have the capacity to store or produce telephone numbers to be called, using a random or sequential number generator, and to call those numbers.” Id. ¶ 13.

Yahoo contends that Mr. Gopalkrishna’s testimony demonstrates that Yahoo’s Email SMS System does not constitute an ATDS under the TCPA, because a system that does not have the capacity to store or produce telephone numbers to be called by using a random or sequential generator cannot satisfy the statutory definition.

Plaintiff tries to dispute Mr. Gopalkrishna’s Declaration, by alleging that he contradicted his Declaration in deposition testimony and by submitting their own expert Declaration from Mr. Randall A. Snyder. Plaintiff alleges that Mr. Gopalkrishna’s deposition testimony undercuts the conclusions in his Declaration because he testified that the system does store cellular telephone numbers; the system sends text messages to those cellular telephone numbers automatically, or in

---

5 Plaintiff attached a transcript of Mr. Gopalkrishna’s Deposition, which took place on October 18, 2013. This transcript does not appear to have been designated with an exhibit number, but the Court will refer to the transcript in this memorandum as “Gopalkrishna Dep.”
other words, without human intervention; and that the system uses a queuing program to control
the order in which text messages will be sent and to manage and backlog in sending messages.
ECF 50 (Pl.’s Sur Reply) at 3. Plaintiff also relies on Mr. Snyder’s conclusion that “the
equipment used by the Defendant has the capacity to store or produce cellular telephone numbers
to be called, using a random or sequential number generator, or from a list of telephone
numbers.” ECF 39-9 (“Snyder Decl.”) ¶ 64.

The Court addressed each of these points— the alleged contradiction between Mr.
Gopalkrishna’s deposition testimony and his Declaration as well as Mr. Snyder’s conclusion—at
oral argument.

There, the Court asked Plaintiff’s counsel to cite to a portion of Mr. Gopalkrishna’s
deposition testimony that contradicted his conclusion that the Yahoo Email SMS Service “did
not have the capacity to store or produce telephone numbers to be called, using a random or
sequential number generator, and to call those numbers.” To be sure, Plaintiff’s counsel did cite
portions of the testimony wherein Mr. Gopalkrishna acknowledges that the system stores cellular
telephone numbers, Gopalkrishna Dep. 52:8-15; that the system sent text messages to those
numbers without human intervention, id. 72:20-73:13; and that the system employs a queue
program for text messages, id. 98:2-7. Yahoo does not dispute that its system operated in this
function, nor does Mr. Gopalkrishna’s Declaration present a contrary description of the system’s
capabilities.

However, these acknowledgements do not resolve the crux of the issue: whether the
system had the capacity to “use a random or sequential number generator to store or produce
telephone numbers and then send a text message to those numbers” as required by the TCPA.
Yahoo asserts that its service could not randomly or sequentially generate telephone numbers,
but only sent messages to a user that had authorized them and only when that user received an email. Plaintiff has not offered evidence to dispute Yahoo’s assertion.

Nor does Mr. Snyder’s Declaration raise a material dispute of fact. Mr. Snyder’s definition of the term “sequence” or “sequential” fails to raise a material dispute of fact, since it focuses on the manner in which text messages are sent, not the way in which the numbers are generated.


Further, Mr. Snyder’s conclusion that the equipment used by the Defendant has the capacity to store or produce cellular telephone numbers to be called, using a random or sequential number generator, or from a list of telephone numbers cannot be relied on to dispute Mr. Gopalkrishna’s Declaration. Mr. Snyder conveniently added the addition disjunctive phrase “or from a list of telephone numbers” to his declaration – a phrase that appears nowhere in the statutory definition of an ATDS. Snyder Decl. ¶ 64 (emphasis added). The inclusion of this additional phrase is misleading. Moreover, including this additional language renders Mr. Snyder’s Declaration entirely unreliable on this point, since it does not address the necessary inquiry here: whether Yahoo’s system constitutes an ATDS as defined by the statute.  

6 Mr. Snyder’s Declaration reflects a misunderstanding of the statutory requirements, which require more than simply that the system store telephone numbers and send messages to those numbers without human intervention. Mr. Snyder’s Declaration references the Ninth Circuit in Satterfield, which quoted from Mr. Snyder’s expert report as follows: “[t]he use of stored numbers, randomly generated numbers or sequentially generated numbers used to automatically originate calls is a technical difference without a perceived distinction.” Snyder Decl. ¶ 49 (quoting Satterfield v. Simon & Schuster, Inc., 569 F.3d at 951). This citation to Satterfield is deceptive. The Ninth Circuit, in Satterfield, quoted Mr. Snyder’s report only to recount his opinions, which were in dispute, and specifically noted
As discussed above, Plaintiff has not offered any evidence to show that Yahoo’s system had the capacity to randomly or sequentially generate telephone numbers (as opposed to simply storing telephone numbers), as required by the statutory definition of ATDS. The Court thus finds that Yahoo did not send text messages to Plaintiff via an ATDS and, therefore, judgment must be granted in favor of Yahoo.

2. Unsolicited Telemarketing

Because the Court finds that the Yahoo system is not an ATDS, it need not address whether the text messages sent constituted “unsolicited telemarketing” of the type that Congress sought to limit with the TCPA.

VI. Conclusion

For the foregoing reasons, this Court grants Yahoo’s Motion for Summary Judgment. An appropriate order follows.
LEXMARK INTERNATIONAL, INC. v. STATIC CONTROL COMPONENTS, INC.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

No. 12–873. Argued December 3, 2013—Decided March 25, 2014

Petitioner Lexmark sells the only style of toner cartridges that work with the company's laser printers, but "remanufacturers" acquire and refurbish used Lexmark cartridges to sell in competition with Lexmark's own new and refurbished ones. Lexmark's "Prebate" program gives customers a discount on new cartridges if they agree to return empty cartridges to the company. Each Prebate cartridge has a microchip that disables the empty cartridge unless Lexmark replaces the chip. Respondent Static Control, a maker and seller of components for the remanufacture of Lexmark cartridges, developed a microchip that mimicked Lexmark's. Lexmark sued for copyright infringement, but Static Control counterclaimed, alleging that Lexmark engaged in false or misleading advertising in violation of §43(a) of the Lanham Act, 15 U. S. C. §1125(a), and that its misrepresentations had caused Static Control lost sales and damage to its business reputation. The District Court held that Static Control lacked "prudential standing" to bring the Lanham Act claim, applying a multifactor balancing test the court attributed to Associated Gen. Contractors of Cal., Inc. v. Carpenters, 459 U. S. 519. In reversing, the Sixth Circuit relied on the Second Circuit's "reasonable interest" test.

Held: Static Control has adequately pleaded the elements of a Lanham Act cause of action for false advertising. Pp. 6–22.

(a) The question here is whether Static Control falls within the class of plaintiffs that Congress authorized to sue under §1125(a). To decide that question, this Court must determine the provision's meaning, using traditional principles of statutory interpretation. It is misleading to label this a "prudential standing" question. Lexmark
bases its “prudential standing” arguments on Associated General Contractors, but that case rested on statutory considerations: The Court sought to “ascertain,” as a statutory-interpretation matter, the “scope of the private remedy created by” Congress in §4 of the Clayton Act, and the “class of persons who [could] maintain a private damages action under” that legislatively conferred cause of action, 459 U. S., at 529, 532. And while this Court may have placed the “zone of interests” test that Static Control relies on under the “prudential” rubric in the past, see, e.g., Elk Grove Unified School Dist. v. Newdow, 542 U. S. 1, 12, it does not belong there any more than Associated General Contractors does. Rather, whether a plaintiff comes within the zone of interests requires the Court to determine, using traditional statutory-interpretation tools, whether a legislatively conferred cause of action encompasses a particular plaintiff’s claim. See, e.g., Steel Co. v. Citizens for Better Environment, 523 U. S. 83, 97, and n. 2. Pp. 6–9.

(b) The §1125(a) cause of action extends to plaintiffs who fall within the zone of interests protected by that statute and whose injury was proximately caused by a violation of that statute. Pp. 10–18.

(1) A statutory cause of action is presumed to extend only to plaintiffs whose interests “fall within the zone of interests protected by the law invoked.” Allen v. Wright, 468 U. S. 737, 751. “[T]he breadth of [that] zone . . . varies according to the provisions of law at issue.” Bennett v. Spear, 520 U. S. 154, 163. The Lanham Act includes a detailed statement of its purposes, including, as relevant here, “protect[ing] persons engaged in [commerce within the control of Congress] against unfair competition,” 15 U. S. C. §1127; and “unfair competition” was understood at common law to be concerned with injuries to business reputation and present and future sales. Thus, to come within the zone of interests in a §1125(a) false-advertising suit, a plaintiff must allege an injury to a commercial interest in reputation or sales. Pp. 10–13.

(2) A statutory cause of action is also presumed to be limited to plaintiffs whose injuries are proximately caused by violations of the statute. See, e.g., Holmes v. Securities Investor Protection Corporation, 503 U. S. 258, 268–270. This requirement generally bars suits for alleged harm that is “too remote” from the defendant’s unlawful conduct, such as when the harm is purely derivative of “misfortunes visited upon a third person by the defendant’s acts.” Id., at 268–269. In a sense, all commercial injuries from false advertising are derivative of those suffered by consumers deceived by the advertising. But since the Lanham Act authorizes suit only for commercial injuries, the intervening consumer-deception step is not fatal to the proximate-cause showing the statute requires. Cf. Bridge v. Phoenix Bond
Syllabus

& Indemnity Co., 553 U. S. 639, 656. Thus, a plaintiff suing under §1125(a) ordinarily must show that its economic or reputational injury flows directly from the deception wrought by the defendant’s advertising; and that occurs when deception of consumers causes them to withhold trade from the plaintiff. Pp. 13–15.

(3) Direct application of the zone-of-interests test and the proximate-cause requirement supplies the relevant limits on who may sue under §1125(a). These principles provide better guidance than the multifactor balancing test urged by Lexmark, the direct-competitor test, or the reasonable-interest test applied by the Sixth Circuit. Pp. 15–18.

(c) Under these principles, Static Control comes within the class of plaintiffs authorized to sue under §1125(a). Its alleged injuries—lost sales and damage to its business reputation—fall within the zone of interests protected by the Act, and Static Control sufficiently alleged that its injuries were proximately caused by Lexmark’s misrepresentations. Pp. 18–22.

697 F. 3d 387, affirmed.

SCALIA, J., delivered the opinion for a unanimous Court.
Opinion of the Court


I. Background

Lexmark manufactures and sells laser printers. It also sells toner cartridges for those printers (toner being the powdery ink that laser printers use to create images on paper). Lexmark designs its printers to work only with its own style of cartridges, and it therefore dominates the market for cartridges compatible with its printers. That market, however, is not devoid of competitors. Other businesses, called “remanufacturers,” acquire used Lexmark toner cartridges, refurbish them, and sell them in competition with new and refurbished cartridges sold by Lexmark.

Lexmark would prefer that its customers return their empty cartridges to it for refurbishment and resale, rather than sell those cartridges to a remanufacturer. So Lexmark introduced what it called a “Prebate” program,
which enabled customers to purchase new toner cartridges at a 20-percent discount if they would agree to return the cartridge to Lexmark once it was empty. Those terms were communicated to consumers through notices printed on the toner-cartridge boxes, which advised the consumer that opening the box would indicate assent to the terms—a practice commonly known as “shrinkwrap licensing,” see, e.g., ProCD, Inc. v. Zeidenberg, 86 F. 3d 1447, 1449 (CA7 1996). To enforce the Prebate terms, Lexmark included a microchip in each Prebate cartridge that would disable the cartridge after it ran out of toner; for the cartridge to be used again, the microchip would have to be replaced by Lexmark.

Static Control is not itself a manufacturer or remanufacturer of toner cartridges. It is, rather, “the market leader [in] making and selling the components necessary to remanufacture Lexmark cartridges.” 697 F. 3d 387, 396 (CA6 2012) (case below). In addition to supplying remanufacturers with toner and various replacement parts, Static Control developed a microchip that could mimic the microchip in Lexmark’s Prebate cartridges. By purchasing Static Control’s microchips and using them to replace the Lexmark microchip, remanufacturers were able to refurbish and resell used Prebate cartridges.


“(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or
any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—

“(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

“(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person’s goods, services, or commercial activities,

“shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.”


As relevant to its Lanham Act claim, Static Control alleged two types of false or misleading conduct by Lexmark. First, it alleged that through its Prebate program Lexmark “purposefully misleads end-users” to believe that they are legally bound by the Prebate terms and are thus required to return the Prebate-labeled cartridge to Lexmark after a single use. App. 31, ¶39. Second, it alleged that upon introducing the Prebate program, Lexmark “sent letters to most of the companies in the toner cartridge remanufacturing business” falsely advising those companies that it was illegal to sell refurbished Prebate cartridges and, in particular, that it was illegal to use Static Control’s products to refurbish those cartridges. Id., at 29, ¶35. Static Control asserted that by those
statements, Lexmark had materially misrepresented “the nature, characteristics, and qualities” of both its own products and Static Control’s products. Id., at 43–44, ¶85. It further maintained that Lexmark’s misrepresentations had “proximately caused and [were] likely to cause injury to [Static Control] by diverting sales from [Static Control] to Lexmark,” and had “substantially injured [its] business reputation” by “leading consumers and others in the trade to believe that [Static Control] is engaged in illegal conduct.” Id., at 44, ¶88. Static Control sought treble damages, attorney’s fees and costs, and injunctive relief.1

The District Court granted Lexmark’s motion to dismiss Static Control’s Lanham Act claim. It held that Static Control lacked “prudential standing” to bring that claim, App. to Pet. for Cert. 83, relying on a multifactor balancing test it attributed to Associated Gen. Contractors of Cal., Inc. v. Carpenters, 459 U. S. 519 (1983). The court emphasized that there were “more direct plaintiffs in the form of remanufacturers of Lexmark’s cartridges”; that Static Control’s injury was “remot[el]” because it was a mere “byproduct of the supposed manipulation of consumers’ relationships with remanufacturers”; and that Lexmark’s “alleged intent [was] to dry up spent cartridge supplies at the remanufacturing level, rather than at [Static Control]’s supply level, making remanufacturers Lexmark’s alleged intended target.” App. to Pet. for Cert. 83.

The Sixth Circuit reversed the dismissal of Static Control’s Lanham Act claim. 697 F. 3d, at 423. Taking the lay of the land, it identified three competing approaches to

1Lexmark contends that Static Control’s allegations failed to describe “commercial advertising or promotion” within the meaning of 15 U. S. C. §1125(a)(1)(B). That question is not before us, and we express no view on it. We assume without deciding that the communications alleged by Static Control qualify as commercial advertising or promotion.
determining whether a plaintiff has standing to sue under the Lanham Act. It observed that the Third, Fifth, Eighth, and Eleventh Circuits all refer to “antitrust standing or the [Associated General Contractors] factors in deciding Lanham Act standing,” as the District Court had done. Id., at 410 (citing Conte Bros. Automotive, Inc. v. Quaker State-Slick 50, Inc., 165 F. 3d 221, 233–234 (CA3 1998); Procter & Gamble Co. v. Amway Corp., 242 F. 3d 539, 562–563 (CA5 2001); Gilbert/Robinson, Inc. v. Carrie Beverage-Missouri, Inc., 989 F. 2d 985, 990–991 (CA8 1993); Phoenix of Broward, Inc. v. McDonald’s Corp., 489 F. 3d 1156, 1162–1164 (CA11 2007)). By contrast, “[t]he Seventh, Ninth, and Tenth [Circuits] use a categorical test, permitting Lanham Act suits only by an actual competitor.” 697 F. 3d, at 410 (citing L. S. Heath & Son, Inc. v. AT&T Information Systems, Inc., 9 F. 3d 561, 575 (CA7 1993); Waits, supra, at 1108–1109; Stanfield v. Osborne Industries, Inc., 52 F. 3d 867, 873 (CA10 1995)). And the Second Circuit applies a “‘reasonable interest’ approach,” under which a Lanham Act plaintiff “has standing if the claimant can demonstrate ‘(1) a reasonable interest to be protected against the alleged false advertising and (2) a reasonable basis for believing that the interest is likely to be damaged by the alleged false advertising.’” 697 F. 3d, at 410 (quoting Famous Horse, Inc. v. 5th Avenue Photo Inc., 624 F. 3d 106, 113 (CA2 2010)). The Sixth Circuit applied the Second Circuit’s reasonable-interest test and concluded that Static Control had standing because it “alleged a cognizable interest in its business reputation and sales to remanufacturers and sufficiently alleged that th[o]se interests were harmed by Lexmark’s statements to the remanufacturers that Static Control was engaging in illegal conduct.” 697 F. 3d, at 411.

We granted certiorari to decide “the appropriate analytical framework for determining a party’s standing to maintain an action for false advertising under the Lanham
II. “Prudential Standing”

The parties’ briefs treat the question on which we granted certiorari as one of “prudential standing.” Because we think that label misleading, we begin by clarifying the nature of the question at issue in this case.

From Article III’s limitation of the judicial power to resolving “Cases” and “Controversies,” and the separation-of-powers principles underlying that limitation, we have deduced a set of requirements that together make up the “irreducible constitutional minimum of standing.” *Lujan v. Defenders of Wildlife*, 504 U. S. 555, 560 (1992). The plaintiff must have suffered or be imminently threatened with a concrete and particularized “injury in fact” that is fairly traceable to the challenged action of the defendant and likely to be redressed by a favorable judicial decision. *Ibid.* Lexmark does not deny that Static Control’s allegations of lost sales and damage to its business reputation give it standing under Article III to press its false-advertising claim, and we are satisfied that they do.

Although Static Control’s claim thus presents a case or controversy that is properly within federal courts’ Article III jurisdiction, Lexmark urges that we should decline to adjudicate Static Control’s claim on grounds that are “prudential,” rather than constitutional. That request is in some tension with our recent reaffirmation of the principle that “a federal court’s ‘obligation’ to hear and decide” cases within its jurisdiction “is ‘virtually unflagging.’” *Sprint Communications, Inc. v. Jacobs*, 571 U. S. ____ (2013) (slip op., at 6) (quoting *Colorado River Water Con-

2 Other aspects of the parties’ sprawling litigation, including Lexmark’s claims under federal copyright and patent law and Static Control’s claims under federal antitrust and North Carolina unfair-competition law, are not before us. Our review pertains only to Static Control’s Lanham Act claim.
In recent decades, however, we have adverted to a “prudential” branch of standing, a doctrine not derived from Article III and “not exhaustively defined” but encompassing (we have said) at least three broad principles: “the general prohibition on a litigant’s raising another person’s legal rights, the rule barring adjudication of generalized grievances more appropriately addressed in the representative branches, and the requirement that a plaintiff’s complaint fall within the zone of interests protected by the law invoked.” Elk Grove Unified School Dist. v. Newdow, 542 U. S. 1, 12 (2004) (quoting Allen v. Wright, 468 U. S. 737, 751 (1984)).

Lexmark bases its “prudential standing” arguments chiefly on Associated General Contractors, but we did not describe our analysis in that case in those terms. Rather, we sought to “ascertain,” as a matter of statutory interpretation, the “scope of the private remedy created by” Congress in §4 of the Clayton Act, and the “class of persons who [could] maintain a private damages action under” that legislatively conferred cause of action. 459 U. S., at 529, 532. We held that the statute limited the class to plaintiffs whose injuries were proximately caused by a defendant’s antitrust violations. Id., at 532–533. Later decisions confirm that Associated General Contractors rested on statutory, not “prudential,” considerations. See, e.g., Holmes v. Securities Investor Protection Corporation, 503 U. S. 258, 265–268 (1992) (relying on Associated General Contractors in finding a proximate-cause requirement in the cause of action created by the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U. S. C. §1964(c)); Anza v. Ideal Steel Supply Corp., 547 U. S. 451, 456 (2006) (affirming that Holmes “relied on a careful interpretation of §1964(c”). Lexmark’s arguments thus do not deserve the “prudential” label.

Static Control, on the other hand, argues that we should
measure its “prudential standing” by using the zone-of-interests test. Although we admittedly have placed that test under the “prudential” rubric in the past, see, e.g., Elk Grove, supra, at 12, it does not belong there any more than Associated General Contractors does. Whether a plaintiff comes within “the ‘zone of interests’” is an issue that requires us to determine, using traditional tools of statutory interpretation, whether a legislatively conferred cause of action encompasses a particular plaintiff’s claim. See Steel Co. v. Citizens for Better Environment, 523 U. S. 83, 97, and n. 2 (1998); Clarke v. Securities Industry Assn., 479 U. S. 388, 394–395 (1987); Holmes, supra, at 288 (SCALIA, J., concurring in judgment). As Judge Silberman of the D. C. Circuit recently observed, “‘prudential standing’ is a misnomer” as applied to the zone-of-interests analysis, which asks whether “this particular class of persons ha[s] a right to sue under this substantive statute.” Association of Battery Recyclers, Inc. v. EPA, 716 F. 3d 667, 675–676 (2013) (concurring opinion).3

3The zone-of-interests test is not the only concept that we have previously classified as an aspect of “prudential standing” but for which, upon closer inspection, we have found that label inapt. Take, for example, our reluctance to entertain generalized grievances—i.e., suits “claiming only harm to [the plaintiff’s] and every citizen’s interest in proper application of the Constitution and laws, and seeking relief that no more directly and tangibly benefits him than it does the public at large.” Lujan v. Defenders of Wildlife, 504 U. S. 555, 573–574 (1992). While we have at times grounded our reluctance to entertain such suits in the “counsels of prudence” (albeit counsels “close[ly] relat[ed] to the policies reflected in” Article III), Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U. S. 464, 475 (1982), we have since held that such suits do not present constitutional “cases” or “controversies.” See, e.g., Lance v. Coffman, 549 U. S. 437, 439 (2007) (per curiam); DaimlerChrysler Corp. v. Cuno, 547 U. S. 332, 344–346 (2006); Defenders of Wildlife, supra, at 573–574. They are barred for constitutional reasons, not “prudential” ones. The limitations on third-party standing are harder to classify; we have observed that third-party standing is “closely related to the question
In sum, the question this case presents is whether Static Control falls within the class of plaintiffs whom Congress has authorized to sue under §1125(a). In other words, we ask whether Static Control has a cause of action under the statute. That question requires us to determine the meaning of the congressionally enacted provision creating a cause of action. In doing so, we apply traditional principles of statutory interpretation. We do not ask whether in our judgment Congress should have authorized Static Control’s suit, but whether Congress in fact did so. Just as a court cannot apply its independent policy judgment to recognize a cause of action that Congress has denied, see Alexander v. Sandoval, 532 U. S. 275, 286–287 (2001), it cannot limit a cause of action that Congress has created merely because “prudence” dictates.

4We have on occasion referred to this inquiry as “statutory standing” and treated it as effectively jurisdictional. See, e.g., Steel Co. v. Citizens for Better Environment, 523 U. S. 83, 97, and n. 2 (1998); cases cited id., at 114–117 (Stevens, J., concurring in judgment). That label is an improvement over the language of “prudential standing,” since it correctly places the focus on the statute. But it, too, is misleading, since “the absence of a valid (as opposed to arguable) cause of action does not implicate subject-matter jurisdiction, i.e., the court’s statutory or constitutional power to adjudicate the case.” Verizon Md. Inc. v. Public Serv. Comm’n of Md., 535 U. S. 635, 642–643 (2002) (quoting Steel Co., supra, at 89); see also Grocery Mfrs. Assn. v. EPA, 693 F. 3d 169, 183–185 (Kavanaugh, J., dissenting), and cases cited therein; Pathak, Statutory Standing and the Tyranny of Labels, 62 Okla. L. Rev. 89, 106 (2009).
III. Static Control's Right To Sue Under §1125(a)

Thus, this case presents a straightforward question of statutory interpretation: Does the cause of action in §1125(a) extend to plaintiffs like Static Control? The statute authorizes suit by “any person who believes that he or she is likely to be damaged” by a defendant’s false advertising. §1125(a)(1). Read literally, that broad language might suggest that an action is available to anyone who can satisfy the minimum requirements of Article III. No party makes that argument, however, and the “unlikelihood that Congress meant to allow all factually injured plaintiffs to recover persuades us that [§1125(a)] should not get such an expansive reading.” *Holmes*, 503 U. S., at 266 (footnote omitted). We reach that conclusion in light of two relevant background principles already mentioned: zone of interests and proximate causality.

A. Zone of Interests

First, we presume that a statutory cause of action extends only to plaintiffs whose interests “fall within the zone of interests protected by the law invoked.” *Allen*, 468 U. S., at 751. The modern “zone of interests” formulation originated in *Association of Data Processing Service Organizations, Inc. v. Camp*, 397 U. S. 150 (1970), as a limitation on the cause of action for judicial review conferred by the Administrative Procedure Act (APA). We have since made clear, however, that it applies to all statutorily created causes of action; that it is a “requirement of general application”; and that Congress is presumed to “legislat[e] against the background of” the zone-of-interests limitation, “which applies unless it is expressly negated.” *Bennett v. Spear*, 520 U. S. 154, 163 (1997); see also *Holmes, supra*, at 287–288 (SCALIA, J., concurring in judgment). It is “perhaps more accurat[e],” though not very different as a practical matter, to say that the limitation *always* applies and is never negated, but that our
analysis of certain statutes will show that they protect a more-than-usually “expansive” range of interests. Bennett, supra, at 164. The zone-of-interests test is therefore an appropriate tool for determining who may invoke the cause of action in §1125(a).5

We have said, in the APA context, that the test is not “‘especially demanding,’” Match-E-Be-Nash-She-Wish Band of Pottawatomie Indians v. Patchak, 567 U. S. ___, ___ (2012) (slip op., at 15). In that context we have often “conspicuously included the word ‘arguably’ in the test to indicate that the benefit of any doubt goes to the plaintiff,” and have said that the test “forecloses suit only when a plaintiff’s ‘interests are so marginally related to or inconsistent with the purposes implicit in the statute that it cannot reasonably be assumed that’” Congress authorized that plaintiff to sue. Id., at ___ (slip op., at 15–16). That lenient approach is an appropriate means of preserving the flexibility of the APA’s omnibus judicial-review provision, which permits suit for violations of numerous statutes of varying character that do not themselves include causes of action for judicial review. “We have made clear, however, that the breadth of the zone of interests varies according to the provisions of law at issue, so that what comes within the zone of interests of a statute for purposes of obtaining judicial review of administrative action under

5Although we announced the modern zone-of-interests test in 1971, its roots lie in the common-law rule that a plaintiff may not recover under the law of negligence for injuries caused by violation of a statute unless the statute “is interpreted as designed to protect the class of persons in which the plaintiff is included, against the risk of the type of harm which has in fact occurred as a result of its violation.” W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser and Keeton on Law of Torts §36, pp. 229–230 (5th ed. 1984); see cases cited id., at 222–227; Gorris v. Scott, [1874] 9 L. R. Exch. 125 (Eng.). Statutory causes of action are regularly interpreted to incorporate standard common-law limitations on civil liability—the zone-of-interests test no less than the requirement of proximate causation, see Part III–B, infra.
the ““generous review provisions”” of the APA may not do so for other purposes.” Bennett, supra, at 163 (quoting Clarke, 479 U. S., at 400, n. 16, in turn quoting Data Processing, supra, at 156).

Identifying the interests protected by the Lanham Act, however, requires no guesswork, since the Act includes an “unusual, and extraordinarily helpful,” detailed statement of the statute’s purposes. H. B. Halicki Productions v. United Artists Communications, Inc., 812 F. 2d 1213, 1214 (CA9 1987). Section 45 of the Act, codified at 15 U. S. C. §1127, provides:

“The intent of this chapter is to regulate commerce within the control of Congress by making actionable the deceptive and misleading use of marks in such commerce; to protect registered marks used in such commerce from interference by State, or territorial legislation; to protect persons engaged in such commerce against unfair competition; to prevent fraud and deception in such commerce by the use of reproductions, copies, counterfeits, or colorable imitations of registered marks; and to provide rights and remedies stipulated by treaties and conventions respecting trademarks, trade names, and unfair competition entered into between the United States and foreign nations.”

Most of the enumerated purposes are relevant to false-association cases; a typical false-advertising case will implicate only the Act’s goal of “protect[ing] persons engaged in [commerce within the control of Congress] against unfair competition.” Although “unfair competition” was a “plastic” concept at common law, Ely-Norris Safe Co. v. Mosler Safe Co., 7 F. 2d 603, 604 (CA2 1925) (L. Hand, J.), it was understood to be concerned with injuries to business reputation and present and future sales. See Rogers, Book Review, 39 Yale L. J. 297, 299
Opinion of the Court

We thus hold that to come within the zone of interests in a suit for false advertising under §1125(a), a plaintiff must allege an injury to a commercial interest in reputation or sales. A consumer who is hoodwinked into purchasing a disappointing product may well have an injury-in-fact cognizable under Article III, but he cannot invoke the protection of the Lanham Act—a conclusion reached by every Circuit to consider the question. See Colligan v. Activities Club of N. Y., Ltd., 442 F. 2d 686, 691–692 (CA2 1971); Serbin v. Ziebart Int’l Corp., 11 F. 3d 1163, 1177 (CA3 1993); Made in the USA Foundation v. Phillips Foods, Inc., 365 F. 3d 278, 281 (CA4 2004); Procter & Gamble Co., 242 F. 3d, at 563–564; Barrus v. Sylvania, 55 F. 3d 468, 470 (CA9 1995); Phoenix of Broward, 489 F. 3d, at 1170. Even a business misled by a supplier into purchasing an inferior product is, like consumers generally, not under the Act’s aegis.

B. Proximate Cause

Second, we generally presume that a statutory cause of action is limited to plaintiffs whose injuries are proximately caused by violations of the statute. For centuries, it has been “a well established principle of [the common] law, that in all cases of loss, we are to attribute it to the proximate cause, and not to any remote cause.” Waters v. Merchants’ Louisville Ins. Co., 11 Pet. 213, 223 (1837); see Holmes, 503 U. S., at 287 (SCALIA, J., concurring in judgment). That venerable principle reflects the reality that “the judicial remedy cannot encompass every conceivable harm that can be traced to alleged wrongdoing.” Associated Gen. Contractors, 459 U. S., at 536. Congress, we assume, is familiar with the common-law rule and does not mean to displace it sub silentio. We have thus construed federal causes of action in a variety of contexts to
incorporate a requirement of proximate causation. See, e.g., *Dura Pharmaceuticals, Inc. v. Broudo*, 544 U. S. 336, 346 (2005) (securities fraud); *Holmes*, *supra*, at 268–270 (RICO); *Associated Gen. Contractors, supra*, at 529–535 (Clayton Act). No party disputes that it is proper to read §1125(a) as containing such a requirement, its broad language notwithstanding.

The proximate-cause inquiry is not easy to define, and over the years it has taken various forms; but courts have a great deal of experience applying it, and there is a wealth of precedent for them to draw upon in doing so. See *Exxon Co., U. S. A. v. Sofec, Inc.*, 517 U. S. 830, 838–839 (1996); *Pacific Operators Offshore, LLP v. Valladolid*, 565 U. S. __, ___ (2012) (SCALIA, J., concurring in part and concurring in judgment) (slip op., at 3). Proximate-cause analysis is controlled by the nature of the statutory cause of action. The question it presents is whether the harm alleged has a sufficiently close connection to the conduct the statute prohibits.

Put differently, the proximate-cause requirement generally bars suits for alleged harm that is “too remote” from the defendant’s unlawful conduct. That is ordinarily the case if the harm is purely derivative of “misfortunes visited upon a third person by the defendant’s acts.” *Holmes, supra*, at 268–269; see, e.g., *Hemi Group, LLC v. City of New York*, 559 U. S. 1, 10–11 (2010). In a sense, of course, all commercial injuries from false advertising are derivative of those suffered by consumers who are deceived by the advertising; but since the Lanham Act authorizes suit only for commercial injuries, the intervening step of consumer deception is not fatal to the showing of proximate causation required by the statute. See *Harold H. Huggins Realty, Inc. v. FNC, Inc.*, 634 F. 3d 787, 800–801 (CA5 2011). That is consistent with our recognition that under common-law principles, a plaintiff can be directly injured by a misrepresentation even where “a third party, and not

We thus hold that a plaintiff suing under §1125(a) ordinarily must show economic or reputational injury flowing directly from the deception wrought by the defendant’s advertising; and that that occurs when deception of consumers causes them to withhold trade from the plaintiff. That showing is generally not made when the deception produces injuries to a fellow commercial actor that in turn affect the plaintiff. For example, while a competitor who is forced out of business by a defendant’s false advertising generally will be able to sue for its losses, the same is not true of the competitor’s landlord, its electric company, and other commercial parties who suffer merely as a result of the competitor’s “inability to meet [its] financial obligations.” Anza, 547 U. S., at 458.6

C. Proposed Tests

At oral argument, Lexmark agreed that the zone of interests and proximate causation supply the relevant background limitations on suit under §1125(a). See Tr. of Oral Arg. 4–5, 11–12, 17–18. But it urges us to adopt, as the optimal formulation of those principles, a multifactor balancing test derived from Associated General Contrac-

6Proximate causation is not a requirement of Article III standing, which requires only that the plaintiff’s injury be fairly traceable to the defendant’s conduct. Like the zone-of-interests test, see supra, at 8–9, and nn. 3–4, it is an element of the cause of action under the statute, and so is subject to the rule that “the absence of a valid (as opposed to arguable) cause of action does not implicate subject-matter jurisdiction.” Steel Co., 523 U. S., at 89. But like any other element of a cause of action, it must be adequately alleged at the pleading stage in order for the case to proceed. See Ashcroft v. Iqbal, 556 U. S. 662, 678–679 (2009). If a plaintiff’s allegations, taken as true, are insufficient to establish proximate causation, then the complaint must be dismissed; if they are sufficient, then the plaintiff is entitled to an opportunity to prove them.
tors. In the alternative, it asks that we adopt a categorical test permitting only direct competitors to sue for false advertising. And although neither party urges adoption of the “reasonable interest” test applied below, several amici do so. While none of those tests is wholly without merit, we decline to adopt any of them. We hold instead that a direct application of the zone-of-interests test and the proximate-cause requirement supplies the relevant limits on who may sue.

The balancing test Lexmark advocates was first articulated by the Third Circuit in Conte Bros. and later adopted by several other Circuits. Conte Bros. identified five relevant considerations:

“(1) The nature of the plaintiff’s alleged injury: Is the injury of a type that Congress sought to redress in providing a private remedy for violations of the [Lanham Act]?

“(2) The directness or indirectness of the asserted injury.

“(3) The proximity or remoteness of the party to the alleged injurious conduct.

“(4) The speculativeness of the damages claim.

“(5) The risk of duplicative damages or complexity in apportioning damages.” 165 F. 3d, at 233 (citations and internal quotation marks omitted).

This approach reflects a commendable effort to give content to an otherwise nebulous inquiry, but we think it slightly off the mark. The first factor can be read as requiring that the plaintiff’s injury be within the relevant zone of interests and the second and third as requiring (somewhat redundantly) proximate causation; but it is not correct to treat those requirements, which must be met in every case, as mere factors to be weighed in a balance. And the fourth and fifth factors are themselves problematic. “[T]he difficulty that can arise when a court attempts
to ascertain the damages caused by some remote action” is a “motivating principle” behind the proximate-cause requirement, Anza, supra, at 457–458; but potential difficulty in ascertaining and apportioning damages is not, as Conte Bros. might suggest, an independent basis for denying standing where it is adequately alleged that a defendant’s conduct has proximately injured an interest of the plaintiff’s that the statute protects. Even when a plaintiff cannot quantify its losses with sufficient certainty to recover damages, it may still be entitled to injunctive relief under §1116(a) (assuming it can prove a likelihood of future injury) or disgorgement of the defendant’s ill-gotten profits under §1117(a). See TrafficSchool.com, Inc. v. Edriver Inc., 653 F. 3d 820, 831 (CA9 2011); Johnson & Johnson v. Carter-Wallace, Inc., 631 F. 2d 186, 190 (CA2 1980). Finally, experience has shown that the Conte Bros. approach, like other open-ended balancing tests, can yield unpredictable and at times arbitrary results. See, e.g., Tushnet, Running the Gamut from A to B: Federal Trademark and False Advertising Law, 159 U. Pa. L. Rev. 1305, 1376–1379 (2011).

In contrast to the multifactor balancing approach, the direct-competitor test provides a bright-line rule; but it does so at the expense of distorting the statutory language. To be sure, a plaintiff who does not compete with the defendant will often have a harder time establishing proximate causation. But a rule categorically prohibiting all suits by noncompetitors would read too much into the Act’s reference to “unfair competition” in §1127. By the time the Lanham Act was adopted, the common-law tort of unfair competition was understood not to be limited to actions between competitors. One leading authority in the field wrote that “there need be no competition in unfair competition,” just as “[t]here is no soda in soda water, no grapes in grape fruit, no bread in bread fruit, and a clothes horse is not a horse but is good enough to hang things
on.” Rogers, 39 Yale L. J., at 299; accord, Vogue Co. v. Thompson-Hudson Co., 300 F. 509, 512 (CA6 1924); 1 H. Nims, The Law of Unfair Competition and Trade-Marks, p. vi (4th ed. 1947); 2 id., at 1194–1205. It is thus a mistake to infer that because the Lanham Act treats false advertising as a form of unfair competition, it can protect only the false-advertiser’s direct competitors.

Finally, there is the “reasonable interest” test applied by the Sixth Circuit in this case. As typically formulated, it requires a commercial plaintiff to “demonstrate (1) a reasonable interest to be protected against the alleged false advertising and (2) a reasonable basis for believing that the interest is likely to be damaged by the alleged false advertising.” 697 F. 3d, at 410 (quoting Famous Horse, 624 F. 3d, at 113). A purely practical objection to the test is that it lends itself to widely divergent application. Indeed, its vague language can be understood as requiring only the bare minimum of Article III standing. The popularity of the multifactor balancing test reflects its appeal to courts tired of “grappling with defining” the “reasonable interest” test “with greater precision.” Conte Bros., 165 F. 3d, at 231. The theoretical difficulties with the test are even more substantial: The relevant question is not whether the plaintiff’s interest is “reasonable,” but whether it is one the Lanham Act protects; and not whether there is a “reasonable basis” for the plaintiff’s claim of harm, but whether the harm alleged is proximately tied to the defendant’s conduct. In short, we think the principles set forth above will provide clearer and more accurate guidance than the “reasonable interest” test.

IV. Application

Applying those principles to Static Control’s false-advertising claim, we conclude that Static Control comes within the class of plaintiffs whom Congress authorized to sue under §1125(a).
To begin, Static Control’s alleged injuries—lost sales and damage to its business reputation—are injuries to precisely the sorts of commercial interests the Act protects. Static Control is suing not as a deceived consumer, but as a “person engaged in” “commerce within the control of Congress” whose position in the marketplace has been damaged by Lexmark’s false advertising. §1127. There is no doubt that it is within the zone of interests protected by the statute.

Static Control also sufficiently alleged that its injuries were proximately caused by Lexmark’s misrepresentations. This case, it is true, does not present the “classic Lanham Act false-advertising claim” in which “‘one competitor[r] directly injure[s] another by making false statements about his own goods [or the competitor’s goods] and thus inducing customers to switch.’” Harold H. Huggins Realty, 634 F. 3d, at 799, n. 24. But although diversion of sales to a direct competitor may be the paradigmatic direct injury from false advertising, it is not the only type of injury cognizable under §1125(a). For at least two reasons, Static Control’s allegations satisfy the requirement of proximate causation.

First, Static Control alleged that Lexmark disparaged its business and products by asserting that Static Control’s business was illegal. See 697 F. 3d, at 411, n. 10 (noting allegation that Lexmark “directly target[ed] Static Control” when it “falsely advertised that Static Control infringed Lexmark’s patents”). When a defendant harms a plaintiff’s reputation by casting aspersions on its business, the plaintiff’s injury flows directly from the audience’s belief in the disparaging statements. Courts have therefore afforded relief under §1125(a) not only where a defendant denigrates a plaintiff’s product by name, see, e.g., McNeilab, Inc. v. American Home Prods. Corp., 848 F. 2d 34, 38 (CA2 1988), but also where the defendant damages the product’s reputation by, for example, equat-
ing it with an inferior product, see, e.g., *Camel Hair and Cashmere Inst. of Am., Inc. v. Associated Dry Goods Corp.*, 799 F. 2d 6, 7–8, 11–12 (CA1 1986); *PPX Enterprises, Inc. v. Audiofidelity, Inc.*, 746 F. 2d 120, 122, 125 (CA2 1984). Traditional proximate-causation principles support those results: As we have observed, a defendant who “seeks to promote his own interests by telling a known falsehood to or about the plaintiff or his product” may be said to have proximately caused the plaintiff’s harm. *Bridge*, 553 U. S., at 657 (quoting Restatement (Second) of Torts §870, Comment h (1977); emphasis added in *Bridge*).

The District Court emphasized that Lexmark and Static Control are not direct competitors. But when a party claims reputational injury from disparagement, competition is not required for proximate cause; and that is true even if the defendant’s aim was to harm its immediate competitors, and the plaintiff merely suffered collateral damage. Consider two rival carmakers who purchase airbags for their cars from different third-party manufacturers. If the first carmaker, hoping to divert sales from the second, falsely proclaims that the airbags used by the second carmaker are defective, both the second carmaker and its airbag supplier may suffer reputational injury, and their sales may decline as a result. In those circumstances, there is no reason to regard either party’s injury as derivative of the other’s; each is directly and independently harmed by the attack on its merchandise.

In addition, Static Control adequately alleged proximate causation by alleging that it designed, manufactured, and sold microchips that both (1) were necessary for, and (2) had no other use than, refurbishing Lexmark toner cartridges. See App. 13, ¶31; id., at 37, ¶54. It follows

7 We understand this to be the thrust of both sides’ allegations concerning Static Control’s design and sale of specialized microchips for the specific purpose of enabling the remanufacture of Lexmark’s
from that allegation that any false advertising that reduced the remanufacturers’ business necessarily injured Static Control as well. Taking Static Control’s assertions at face value, there is likely to be something very close to a 1:1 relationship between the number of refurbished Prebate cartridges sold (or not sold) by the remanufacturers and the number of Prebate microchips sold (or not sold) by Static Control. “Where the injury alleged is so integral an aspect of the [violation] alleged, there can be no question” that proximate cause is satisfied. *Blue Shield of Va. v. McCready*, 457 U. S. 465, 479 (1982).

To be sure, on this view, the causal chain linking Static Control’s injuries to consumer confusion is not direct, but includes the intervening link of injury to the remanufacturers. Static Control’s allegations therefore might not support standing under a strict application of the “‘general tendency’” not to stretch proximate causation “‘beyond the first step.’” *Holmes*, 503 U. S., at 271. But the reason for that general tendency is that there ordinarily is a “discontinuity” between the injury to the direct victim and the injury to the indirect victim, so that the latter is not surely attributable to the former (and thus also to the defendant’s conduct), but might instead have resulted from “any number of [other] reasons.” *Anza*, 547 U. S., at 458–459. That is not the case here. Static Control’s allegations suggest that if the remanufacturers sold 10,000 fewer refurbished cartridges because of Lexmark’s false advertising, then it would follow more or less automatically that Static Control sold 10,000 fewer microchips for the same reason, without the need for any “speculative . . . proceedings” or “intricate, uncertain inquiries.” *Id.*, at 459–460. In these relatively unique circumstances, the remanufacturers are not “more immediate victim[s]” than Static Control. *Bridge, supra*, at 658.

Prebate cartridges.
Although we conclude that Static Control has alleged an adequate basis to proceed under §1125(a), it cannot obtain relief without evidence of injury proximately caused by Lexmark’s alleged misrepresentations. We hold only that Static Control is entitled to a chance to prove its case.

* * *

To invoke the Lanham Act’s cause of action for false advertising, a plaintiff must plead (and ultimately prove) an injury to a commercial interest in sales or business reputation proximately caused by the defendant’s misrepresentations. Static Control has adequately pleaded both elements. The judgment of the Court of Appeals is affirmed.

It is so ordered.
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

C.M.D., et al.,

v.

FACEBOOK, INC.,

Plaintiffs,

Defendant.

ORDER GRANTING MOTION TO DISMISS SECOND AMENDED COMPLAINT

I. INTRODUCTION

This putative class action, originally filed in the Southern District of Illinois, initially advanced a single claim. Plaintiffs sought statutory damages for defendant Facebook’s alleged commercial misappropriation of the names and likenesses of minors who utilize the Facebook social network website. In connection with a motion to intervene these plaintiffs brought in Fraley v. Facebook, C 11-01726 RS, counsel represented that a settlement of that action would, effectively, foreclose the claims alleged here. The named plaintiffs, however, exercised their right to opt-out of the Fraley settlement, and after that settlement received final approval, they recast their claims in this action. At least at this juncture, Facebook is not contending the Fraley settlement provides a basis for dismissal, although it does assert the settlement will limit membership in the putative class here to those who opted out in Fraley.
The operative Second Amended Complaint ("SAC") sets out four counts. The first two counts seek declaratory relief, and the latter two assert claims under an Illinois statute prohibiting the “use of an individual’s identity for commercial purposes” without prior written consent. For reasons explained below, all four claims require plaintiffs to have a tenable basis for challenging the enforceability of Facebook’s Statement of Rights and Responsibilities (“SRRs”) that purport to govern the use of the Facebook site. Because plaintiffs have not articulated a viable legal theory on which the SRRs could be found unenforceable, the complaint must be dismissed.

II. BACKGROUND

This action, like Fraley, involves practices by which Facebook utilizes the names and profile pictures of its users in ways that arguably constitute advertising for various third parties. The putative plaintiff class in this action is composed solely of minors; a subclass in Fraley. Facebook insists it does nothing more than take information its users have voluntarily shared with their Facebook friends, and republish it to those same friends, “sometimes alongside a related advertisement.”

Before arriving at that question, the threshold issue is whether Facebook’s SRRs are legally enforceable. Plaintiffs effectively concede that if the SRRs are enforceable, they include written consent to the challenged use of names and profile photos, such that the underlying damages claims are not viable.

III. LEGAL STANDARD

A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). While “detailed factual allegations are not required,” a complaint must have sufficient factual allegations to “state a claim to relief that is plausible on its face.” Ashcroft v. Iqbal, 566 U.S. 652, 678 (2009) (citing Bell Atlantic v. Twombly, 550 U.S. 544, 570 (2007)). A claim is facially plausible “when the pleaded factual content allows the court to

1 Fraley involved only a Facebook program known as “Sponsored Stories.” This case also includes a program called “Social Ads,” which allows third parties to add their own content to the user material that is displayed.
draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* This standard asks for “more than a sheer possibility that a defendant acted unlawfully.” *Id.* The determination is a context-specific task requiring the court “to draw in its judicial experience and common sense.” *Id.* at 1950.

A motion to dismiss a complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure tests the legal sufficiency of the claims alleged in the complaint. See *Parks Sch. of Bus., Inc. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995). Dismissal under Rule 12(b)(6) may be based on either the “lack of a cognizable legal theory” or on “the absence of sufficient facts alleged under a cognizable legal theory.” *Balistreri v. Pacifica Police Dep’t*, 901 F.2d 696, 699 (9th Cir. 1990).

Here, Facebook’s motion does not take issue with the sufficiency of the facts pleaded *per se*, and instead argues that plaintiff’s legal theory is fatally flawed, for various reasons. As explained below, even though not all of Facebook’s arguments are persuasive, plaintiffs’ basic legal theory is indeed untenable.

IV. DISCUSSION

A. Standing

Facebook first contends plaintiffs lack Article III standing to bring this action, arguing they have failed to present facts showing they suffered any legally cognizable harm from the alleged conduct. While similar general arguments were initially accepted in *Cohen v. Facebook, Inc.*, 2011 WL 5117164, at *3-4 (N.D. Cal. 2011), they were rejected in *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011).

To the extent *Fraley* and *Cohen* are distinguishable from each other, this action has more in common with *Fraley* than it does with *Cohen*. Both here and in *Fraley*, but not in *Cohen*, plaintiffs have alleged that their names and likeness are used to endorse third-party products, companies, and

---

2 Facebook also challenges plaintiffs’ standing under Rule 12(b)(1). A court may dismiss a claim under that rule based on a lack of subject matter jurisdiction, and the motion may attack either the complaint on its face or the existence of jurisdiction in fact. See *Thornhill Publ’g Co. v. Gen. Tel. & Elecs. Corp.*, 594 F.2d 730, 732-33 (9th Cir. 1979). If a complaint does not establish standing under Article III of the U.S. Constitution, a federal court does not have subject matter jurisdiction to hear the case. See *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 101-02 (1998).
brands, with a resulting inference that those endorsements have “concrete, measurable, and provable value in the economy at large.” *Fraley*, 830 F. Supp. 2d at 799.

Furthermore, as *Fraley* points out, “a plaintiff may be able to establish constitutional injury in fact by pleading violation of a right conferred by statute, so long as she can allege that the injury she suffered was specific to her.” *Id.* The Ninth Circuit applied this principle in *Edwards v First Am. Corp.*, 610 F.3d 514 (9th Cir. 2010), finding that a plaintiff who alleged a statutory violation of the Real Estate Settlement Procedures Act of 1974, 12 U.S.C. § 2607, had standing despite her inability to allege that she had actually been overcharged for any services.

Facebook argues *Edwards* is not controlling here because, in Facebook’s view, the Illinois statutory claims advanced by plaintiffs are not viable given the choice of law provisions of the SRRs. That argument puts the merits cart before the standing horse. Plaintiffs’ claim is that the SRRs are not enforceable and that Facebook has therefore violated the Illinois statutes. Standing to determine whether the Illinois law applies and has been violated does not depend on the claim being proven meritorious in the end.

Finally, Facebook asserts *Edwards* was simply “wrongly decided” insofar as it endorses standing absent some actual injury beyond the mere fact of a statutory violation. Any argument that *Edwards* should be revisited must be presented to the Circuit court, not here. Accordingly, dismissal for lack of standing would not be warranted.

B. Count I—Declaratory Relief re enforceability of SRRs

Plaintiffs contend the consent provisions in the SRRs are legally unenforceable as to the putative class of minors because they represent a type of contract into which a minor cannot legally enter under California Family Code §6701, and are therefore *void ab initio*. Alternatively, plaintiffs argue the SRRs are *voidable* under Family Code §6710.³

³ The complaint refers to “Family Code §6702,” which does not exist. There appears to be no dispute that plaintiffs intended to invoke Family Code §6710, and can be deemed to have done so.
Family Code §6700 sets out the general rule:

Except as provided in Section 6701, a minor may make a contract in the same manner as an adult, subject to the power of disaffirmance under Chapter 2 (commencing with Section 6710) . . . .

Accordingly, while contracts made by minors generally may be disaffirmed (or, in plaintiffs’ words, are “voidable”), provided the conditions set out in section 6710 and following sections are met, the basic presumption is that minors do have the power to enter into binding contracts except as provided in §6701.

Plaintiffs’ arguments largely flow from an opposite, and incorrect presumption, that minors generally do not have the power to contract. As articulated during oral argument, plaintiffs contend the rule is a “[m]inor cannot contract,” with only “exceptions for necessities.” Plaintiffs thus would narrow the circumstances in which minors’ contracts are allowed, and would construe broadly the prohibitions against certain specific types of contracts described in §6701. This turns statutory construction on its head. Because the general rule is set forth in §6700, it is the exceptions set out in §6701 that must be construed narrowly, if anything. See Barnes v. Chamberlain, 147 Cal.App.3d 762, 767(1983) (“Exceptions to the general rule of a statute are to be strictly construed. In interpreting exceptions to the general statute courts include only those circumstances which are within the words and reason of the exception . . . . One seeking to be excluded from the sweep of the general statute must establish that the exception applies.”)

Turning then to the exceptions set out in §6701, plaintiffs have not met their burden to establish their applicability. The statute provides:

A minor cannot do any of the following:

(a) Give a delegation of power.
(b) Make a contract relating to real property or any interest therein.
(c) Make a contract relating to any personal property not in the immediate possession or control of the minor.

Plaintiffs contend the SRRs violate subdivision (a), (c), or both. They acknowledge that the predecessor to subdivision (a) was enacted to preclude minors from authorizing agents to enter into

4 Additional qualifications, relating to marriages of minors, are not pertinent here.
additional contracts on their behalf. See Hakes Inv. Co. v. Lyons, 166 Cal. 557, 560 (1913) (“it is obvious that the intention of the Legislature . . . . [was to] declare the rule that an infant could not execute contracts through an agent having only a delegated authority executed by the infant.”); see also Morgan v. Morgan, 220 Cal. App. 2d 665, 674-75 (1963) (holding that a child actor’s authorization to his agent to endorse paychecks on his behalf constituted a void delegation of power).

Plaintiffs insist that the provision should not be so narrowly construed as to apply only in cases of formal appointments of agents or other such clear delegations of authority. Even accepting that assumption, plaintiffs have offered no persuasive basis for finding subdivision (a) to be implicated by the SRRs, either generally or with respect to the consent provision plaintiffs are challenging. The consent Facebook users give for use of their names and profile pictures in certain ways on the site simply is not tantamount to appointing Facebook as an agent for users, or to delegating to it any power to be exercised on behalf of those users. While Facebook may obtain “powers” under the SRRs to utilize the names and pictures in certain ways, that is no different from garden-variety rights a contracting party may obtain in a wide variety of contractual settings. Plaintiffs have not shown how it would be a delegation of power within the meaning of the statute. Rather, Facebook users have, in effect, simply granted Facebook the right to use their names in pictures in certain specified situations, in exchange for whatever benefits they may realize from using the Facebook site.

Plaintiffs’ alternative reliance on subdivision (c) is no more persuasive. They acknowledge that the reference to property “in the immediate possession” of the minor supports a conclusion that the section is primarily intended to address tangible personal property. Because they fail to recognize that void contracts are the exception, not the rule, plaintiffs then incorrectly reason that contracts relating to intangible property must fall within subdivision (c). To the contrary, because subdivision (c) is directed at tangible property (as plaintiffs admit), it only renders void certain contracts relating to such property. Regardless of exactly how the rights putative class members hold in their names and profile pictures may be labeled, they cannot be fairly characterized as “personal property not in the immediate possession or control of the minor.”
Plaintiffs essentially agree that the names and profile pictures do not fall within the language of subdivision (c). They err in then concluding the SRRs are void under that subdivision, instead of recognizing that because the subdivision does not apply (and neither do the other subdivisions of §6701), the default is the general rule of §6700—“a minor may make a contract in the same manner as an adult . . . ” Accordingly, plaintiffs have shown no basis for finding the SRRs to be void.

As noted, plaintiffs alternatively argue the SRRs are voidable under Family Code §6710. That section provides:

Except as otherwise provided by statute, a contract of a minor may be disaffirmed by the minor before majority or within a reasonable time afterwards or, in case of the minor's death within that period, by the minor’s heirs or personal representative.

Although this section almost certainly would allow plaintiffs to disaffirm the SRRs, they have never plainly expressed an intent to do so, and they do not dispute that they continued to use their Facebook accounts long after this action was filed. While Plaintiffs argue that a minor may disaffirm a contract without restoring any of the benefits he or she received, they have offered no explanation as to how that principle would somehow retroactively vitiate the consent they had given through the SRRs at the time their names and profile pictures were used. Thus, the possibility that the named plaintiffs and members of the putative class might rely on §6710 to disaffirm the SRRs and close their Facebook accounts does not render viable any of the claims they have pleaded. Because plaintiffs have offered no facts or legal theories upon which they would be entitled to a declaration the SRRs are unenforceable, Count I must be dismissed.5

5 Facebook argues the same result would follow through application of “law of the case,” given the decision made by the transferring district in this action to enforce the venue provisions of the SRRs. Because it is unclear whether all of the prerequisites for application of law of the case doctrine are present here, and because it is a flexible doctrine in any event, proceeding to the merits of the arguments is the preferred course.
C. Count II—Declaratory Relief re preemption under Children’s Online Privacy Protection Act, 15 U.S.C. §6501-6506 ("COPPA")

Plaintiffs seek declaratory relief that their claims are not preempted under COPPA. Facebook argues there is no existing controversy because it is not presently asserting a COPPA preemption defense in this action. Given Facebook’s prior invocation of COPPA, there likely would be a sufficient basis for declaratory relief on the point were there otherwise a live controversy remaining. In light of the disposition of Count I above, however, any declaration in this action regarding possible COPPA preemption would be purely advisory.

D. Counts III and IV—Illinois Right of Publicity Act

Plaintiffs effectively concede that their claims under Illinois law are dependent on a conclusion that the SRRs—which contain a California choice of law provision—are invalid. Accordingly, with the failure of Count I, the claims under Illinois law must also be dismissed.

V. CONCLUSION

The motion to dismiss is granted. Plaintiffs acknowledged at the hearing that the viability of their claims turns on legal arguments, such that no further development of factual allegations would result in a different analysis or outcome, and therefore they do not request leave to amend. A separate judgment will therefore enter.

IT IS SO ORDERED.

Dated: 3/26/14

RICHARD SEEBORG
UNITED STATES DISTRICT JUDGE
IN THE
COURT OF APPEALS OF INDIANA

JEFFREY M. MILLER and
CYNTHIA S. MILLER,
Appellants-Plaintiffs,

vs.

FEDERAL EXPRESS CORPORATION and
500 FESTIVAL, INC.,
Appellees-Defendants.

No. 49A02-1307-PL-619

APPEAL FROM THE MARION SUPERIOR COURT
The Honorable Michael D. Keele, Judge
Cause No. 49D07-1003-PL-014761

April 3, 2014

OPINION – FOR PUBLICATION

MATHIAS, Judge
Jeffrey M. Miller and Cynthia S. Miller (“the Millers”) appeal the Marion Superior Court’s grant of summary judgment in favor of Federal Express Corporation (“FedEx”) and 500 Festival, Inc. (“500 Festival”) on the Millers’ claim of defamation and intentional infliction of emotional distress. The Millers appeal, claiming: (1) that the Defendants failed to preserve evidence, and (2) that the Defendants are not immune from suit under the federal Communications Decency Act.

We affirm.

Facts and Procedural History

From 1994 until his retirement in 2008, Jeffrey Miller (“Miller”) was the president of Junior Achievement of Central Indiana (“JACI”). After his retirement, Miller acted as president of the Experiential Learning and Entrepreneurship Federation (“ELEF”), which is a separate organization from JACI, but which works with JACI. In the spring of 2008, Miller announced a joint project between JACI, ELEF, and Ivy Tech Community College (“Ivy Tech”), which provided for ELEF to construct a culinary school on JACI property which Ivy Tech would then lease. Construction on the building began in 2009, but was stopped in 2010 when the primary financial backers of the project stopped providing the necessary funds. This was allegedly due to defamatory statements made by Jennifer Burk (“Burk”) and Brian Payne (“Payne”), who are co-defendants in the Millers’ current action.¹

¹ Burk succeeded Miller as president of JACI, and Payne was the president of the Central Indiana Community Foundation, Inc. (“CICF”).
What happened next is the focus of the current controversy. On March 18, 2010, the Indianapolis Business Journal (“IBJ”) published an article on its website regarding the allegations and controversy surrounding the construction of the culinary school. Several comments regarding this article were posted to the IBJ website. The Millers allege that several of these comments were defamatory.

One comment, posted by a user with the screen name “JA Fan” on March 19, 2010, read:

The new CEO [Burk] has inherited a mess not of her doing. The former CEO [Miller] and finally-fired VP’s misuse (for their own personal gain) of funds that were dedicated to educating Indiana children are at the very least an embarrassment to the dedicated staff who have continued to push on, and most likely a criminal act. If you were a donor or sponsor in the last decade to these guys, an audit is definitely in order. Hang in there, Jennifer Burk!”

Appellant’s App. pp. 82.

On March 23, 2010, a user with the screen name “Really?” posted a comment which read in relevant part:

Article- “ELEF is the owner (you would have to be to sign construction contracts worth millions) of the N. Keystone building and Junior Achievement’s partner in receiving the $3 million grant. That foundation exists solely to benefit (raise money for) Junior Achievement, and until recently, was overseen by Junior Achievement’s managers (Miller). Junior Achievement took on the culinary school project, under longtime CEO Jeff Miller (because in addition to educating Indiana children in business and financial responsibility, teaching adults to cook for others has long been part of the JA mission. Just call the national office and ask, I’m sure it’s true). He retired but continued to serve as president of the ELEF (money) through last year.” Article cont.- “Miller said his role last year was to raise additional donations for the $7 million culinary school project and oversee day-to-day construction activities.” Does this include paying the contractors? As the fundraiser and key money guy, probably has an eye on revenue and expenses. Article-“I was the project manager, but I didn’t
have any communication about this stopping of money,’ he said.” Comment quote from other post-“what is so depressing and unfair is that the subcontractors were never told the funds were suspended and JACI, ELEF and CICF let them keep working.” Article-“The community foundation informed JA in writing on Nov. 24 that all future payments under the grant would be suspended until ‘issues’ were resolved.” Probably wasn’t the first or only communication. If they told JA, who did not own the building or sign the construction contracts, I’m pretty sure as a tenant with an interest in what’s happening to the building, they would notify the Landlord, President Miller (who did the deal to bring Ivy Tech to the building, who also took money to fund the construction, who was also the “project manager” responsible for day-to-day operations) that his project is going to be halted and his building left in a mess. Now a storied and critical organization is a mess in his wake. Was it the great philosopher, Steve Miller, who said, “Go on, take the money and run!”? Perhaps a relative?

Appellant’s App. pp. 82-83. Another comment was posted on April 6, 2010,2 by someone using the online handle of “Concernd.” This person posted a comment that read, “These guys are crooks (Jeff Miller, Victor George and other parties) and have been robbing from our community using kids as there [sic] hook. I hope they go to jail!!!!” Appellant’s App. p. 84.

During discovery, the Millers learned that the first two comments were made by Dave Wilson (“Wilson”), the vice president of corporate sponsorship at 500 Festival. He used a computer owned by 500 Festival and located at 500 Festival offices to make these comments. The IP address from which these comments were posted was assigned to 500 Festival by AT&T, 500 Festival’s internet service provider (“ISP”). The third comment was made by an unknown person from an IP address assigned to FedEx. The IP address

---

2 By the time of this comment, the Millers had already filed suit against Burk, Payne, and JACI.
was not traceable to any specific user, but instead belonged to one of FedEx’s proxy servers which filtered internet traffic from tens of thousands of FedEx users.

On February 25, 2011, the Millers amended their complaint to add 500 Festival and FedEx as defendants. On November 23, 2011, the Millers served FedEx with interrogatories and requests for production. FedEx objected to the scope of these discovery requests and sought a protective order, which the trial court denied. And after FedEx had responded to the Millers’ discovery, the Millers took issue with the adequacy of FedEx’s response.

On February 21, 2013, FedEx filed a motion for summary judgment. 500 Festival filed a motion for summary judgment one week later, on February 28, 2013. The Millers responded to these motions on April 30, 2013, after having been granted an extension of time in which to reply. In their response, the Millers claimed that they had received inadequate discovery from 500 Festival. The Millers then filed a motion for sanctions against FedEx and 500 Festival on May 22, 2013, claiming that these defendants had spoliated evidence. The trial court held a hearing on the motions for summary judgment on May 22, 2013, and on July 1, 2013, entered summary judgment in favor of FedEx and 500 Festival. The trial court entered a separate order on July 1, 2013, denying the Millers’ motion for sanctions against 500 Festival and entered a similar order denying the Millers’ motion for sanctions against FedEx on July 5, 2013. The Millers now appeal.

**Summary Judgment Standard of Review**

Our standard for reviewing a trial court’s order granting a motion for summary judgment is well settled: a trial court should grant a motion for summary judgment only
when the evidence shows that there is no genuine issue as to any material fact and that
the moving party is entitled to a judgment as a matter of law. Altevogt v. Brand, 963
N.E.2d 1146, 1150 (Ind. Ct. App. 2012) (citing Ind. Trial Rule 56(C)). The trial court’s
grant of a motion for summary judgment comes to us cloaked with a presumption of
validity. Id. “An appellate court reviewing a trial court summary judgment ruling
likewise construes all facts and reasonable inferences in favor of the non-moving party
and determines whether the moving party has shown from the designated evidentiary
matter that there is no genuine issue as to any material fact and that it is entitled to
judgment as a matter of law.” Id. (quoting Dugan v. Mittal Steel USA Inc., 929 N.E.2d
184, 186 (Ind. 2010)). However, a de novo standard of review applies where the dispute
is one of law rather than fact. Id. On appeal, we examine only those materials designated
to the trial court on the motion for summary judgment, and we must affirm the trial
court’s entry of summary judgment if it can be sustained on any theory or basis in the
record. Id.

I. Preservation of Evidence

The Millers first claim that the trial court erred in granting summary judgment
because both of the Defendants failed to preserve evidence for discovery. Specifically,
the Millers refer to certain computer records or files that the Defendants had in their
possession. As noted by the Millers, our supreme court has recognized that:

[Intentional destruction of potential evidence in order to disrupt or defeat
another persons’s right of recovery is highly improper and cannot be
justified. The intentional or negligent destruction or spoliation of evidence
cannot be condoned and threatens the very integrity of our judicial system.
There can be no truth, fairness, or justice in a civil action where relevant]
evidence has been destroyed before trial. Destroying evidence can destroy fairness and justice, for it increases the risk of an erroneous decision on the merits of the underlying cause of action. Destroying evidence can also increase the costs of litigation as parties attempt to reconstruct the destroyed evidence or to develop other evidence, which may be less accessible, less persuasive, or both.

Gribben v. Wal-Mart Stores, Inc., 824 N.E.2d 349, 354 (Ind. 2005) (citations and internal quotations omitted). But there is no independent cause of action in Indiana for spoliation of evidence by a party to the suit. Id. at 355. Instead, Indiana trial courts have considerable discretion to respond to discovery violations with such sanctions “as are just” under Trial Rule 37(B). Also, “intentional first-party spoliation of evidence may be used to establish an inference that the spoliated evidence was unfavorable to the party responsible.” Id. at 351.

Here, in November 2010, before the Millers added FedEx as a defendant, they served FedEx with a non-party discovery request for information regarding the IP address that was used to post one of the comments on the IBJ website. FedEx responded to this request by informing the Millers that the IP address that had been used to post the comment to the IBJ website was that of a proxy server which filtered internet traffic for tens of thousands of users. FedEx also gave the Millers a copy of the FedEx document retention policy for its proxy servers’ logs. This policy explained that such archives are stored for one year. In January 2011, before FedEx was added as a defendant, the proxy server at issue was taken out of service by FedEx in the ordinary course of business. Importantly, the Millers did not thereafter ask FedEx to supplement this response or otherwise complain that the response was inadequate. Instead, the Millers amended their
complaint to add FedEx as a defendant on February 25, 2011. The complaint, however, did not allege that the commenter was a FedEx employee, was authorized to post the comment, or posted the comment in the scope of his or her employment.

By this time, however, the proxy server had been taken out of service. And the server logs from April 6, 2010, the date when the comment was posted to IBJ, were purged on April 6, 2011, shortly after FedEx was served with the Millers’ complaint but pursuant to the retention policy produced by FedEx to the Millers in third-party discovery. Thus, at the time the server logs were destroyed, FedEx had already responded to the Millers’ requests for non-party discovery, and the Millers had not complained of FedEx’s discovery responses. Moreover, FedEx has never denied that the IP address at issue was associated with its server. Nor had the Millers at that time requested that FedEx preserve the server logs. Under these facts and circumstances, we cannot say that the trial court erred by failing to sanction FedEx for failing to preserve the records of the proxy server.

The Millers also complain, however, that FedEx failed to preserve any electronic records until November 15, 2012, which was over a year after FedEx had been added as a defendant. The Millers’ initial, non-party discovery requests were broad—effectively asking FedEx to search for documents relating to the Millers’ claims from all 290,000 FedEx employees. FedEx objected to the breadth of these requests, and on July 11, 2012, sent correspondence to the Millers’ counsel asking for information to help narrow the discovery requests. The Millers did not respond. Eventually, the trial court ordered the parties to meet and resolve the discovery issues after the Millers filed a motion for sanctions due to FedEx’s alleged failure to properly provide discovery. This was done on
November 6 and November 15, 2012. Only then did the Millers limit the scope of their requests to seventeen current and former employees of FedEx who had volunteered for JACI. Thus, once the Millers narrowed their discovery requests to a reasonable scope, FedEx began to preserve records pertaining to these identified employees. Again, under these facts and circumstances, we cannot say that the trial court erred by failing to sanction FedEx for its responsiveness to the Millers’ discovery requests.

With regard to 500 Festival, however, the situation was different. Relatively early on in the discovery process, Wilson was known to be the employee who used 500 Festival’s computer system to post the comments via his Yahoo account. And the Millers added Wilson as a defendant at the same time that they added 500 Festival. Thus, from the beginning of its involvement in this case, 500 Festival knew that one of its employees was also a defendant and had made the comments at the heart of the Millers’ claims. Despite this, 500 Festival made no efforts to preserve the contents of Wilson’s computer. In fact, 500 Festival replaced Wilson’s computer but failed to make a complete archival backup of the contents of the drive(s) on the computer. Instead, it simply relied on its policy that employees save documents to 500 Festival’s file server. It also instructed employees to backup any “computer specific” files to a shared drive on the server prior to the change of computers.

Certainly, the better practice for 500 Festival would have been to preserve the contents of Wilson’s computer, otherwise known as placing a unilateral “litigation hold” on the computer and its contents. The seminal case in electronic discovery is *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003), In *Zubulake*, Judge
Scheindlin recognized the dilemmas posed by the nature of electronic documents, saying that a corporation, upon recognizing the threat of litigation, need not “preserve every shred of paper, every e-mail or electronic document, and every backup tape,” as such a rule would “cripple large corporations . . . that are almost always involved in litigation.”

At the same time, anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary. While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

Id. (citation and internal quotation omitted). Further, “if a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of ‘key players’ to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available.” Id. at 218. Thus, after being added as a defendant and identifying co-defendant Wilson’s computer at issue in the present case, 500 Festival should have taken measures to preserve the contents of his computer.

Still, 500 Festival notes that the Millers failed to send 500 Festival any request to place a “litigation hold” on the content of Wilson’s computer. See Reinbold v. Harris, IP00-0587-C-T/G, 2000 WL 1693792 (S.D. Ind. Nov. 7, 2000) (“Mere ownership of potential evidence, even with knowledge of its relevance to litigation, does not suffice to establish a duty to maintain such evidence.”). Again, if the Millers thought the content of Wilson’s computer was vital to their case, they could have specifically requested that 500
Festival archive the content of Wilson’s computer. Thus, it appears that neither the Millers nor 500 Festival did all that they could have done and should have done in order to preserve the contents of Wilson’s computer. However, we need not pursue the discovery issues concerning the contents of the hard drive on Wilson’s computer, and we do not think that 500 Festival’s failure to preserve the contents of this computer required the trial court to deny summary judgment in favor of 500 Festival. Both of these issues are mooted by the fact that both FedEx and 500 Festival are immune from the claims brought by the Millers.

II. Immunity Under The Communications Decency Act

The trial court granted summary judgment in favor of 500 Festival and FedEx based on its conclusion that these defendants were protected from liability by operation of the federal Communications Decency Act ("CDA"). On appeal, the Millers claim that the trial court’s conclusion was erroneous. Because this is strictly a question of law, our review is de novo. Altevogt, 963 N.E.2d at 1150.

At issue here is Section 230 of the CDA, which provides:

(a) Findings
The Congress finds the following:
(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.
(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy
It is the policy of the United States—
(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material; and
(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for “good samaritan” blocking and screening of offensive material
(1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability
No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).
(d) Obligations of interactive computer service

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

* * *

(f) Definitions

As used in this section:

(1) Internet

The term “Internet” means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term “interactive computer service” means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

The term “information content provider” means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service. . . .


In the leading case on Section 230 immunity, the federal Fourth Circuit Court of Appeals in Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997), noted that:

By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher’s role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions—such as
deciding whether to publish, withdraw, postpone or alter content—are barred.

Id. at 330. The Zeran court also noted that the purpose of Section 230 immunity is not difficult to discern:

Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.

Id.

Thus, Congress made a policy choice not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages. Id. This is so because interactive computer services have millions of users, and the amount of information communicated via interactive computer services is “staggering.” Id. “The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems.” Id. Congress considered the weight of the speech interests implicated and chose to immunize providers of interactive computer services to avoid any restrictive effect. Id. This does not mean, however, that the party who actually posts the defamatory message can escape liability. Id. But Congress made a policy choice not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages. Id. at 330-31.
Other courts have adopted this broad reading of the protections afforded by Section 230(c). See, e.g., Doe v. MySpace, Inc., 528 F.3d 413, 418-19 (5th Cir. 2008) (holding that operator of social media website was protected by Section 230 from suit by minors who were sexually assaulted by men they met on the site); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123-24 (9th Cir. 2003) (holding that an online dating service provider was not liable when an unidentified party posted a false online profile for a popular actress, leading her to receive sexually explicit phone calls, letters, and faxes at home); Batzel v. Smith, 333 F.3d 1018, 1030-31 (9th Cir. 2003) (concluding that operator of a museum security website was protected by Section 230 from suit brought by person allegedly defamed by email posted to the site and its email list because language of Section 230 confers immunity on both providers and users of interactive computer services); Green v. Am. Online (AOL), 318 F.3d 465, 471 (3d Cir. 2003) (holding that web-based service provider was protected by Section 230 from claim by user who claimed he received a computer virus from third party and endured derogatory comments directed at him by other users); Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 984-86 (10th Cir. 2000) (holding that online service provider was immune from defamation claim based on inaccurate stock information). And even those courts which have not interpreted Section 230(c)’s protection as broadly as the Fourth Circuit in Zupan have still acknowledged that a provider of an interactive computer service cannot be liable as a publisher or speaker of information provided by someone else. See Chicago Lawyers’ Comm’n for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008).
Thus, the question before us is whether 500 Festival and FedEx qualify as providers of an “interactive computer service” for purposes of Section 230(c)(1). The Millers argue that neither 500 Festival nor FedEx provided an interactive computer service, but are instead employers providing computer services to their employees via third-party ISPs.

Section 230(f)(2) defines an “interactive computer service” to mean “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.” The Millers acknowledge the case law that has extended Section 230 immunity to websites such as Google, Yahoo, and Microsoft, but claim that it does not extend to employers who provide access to their employees and others to the internet. The cases that have addressed this question, however, have decided otherwise.

In Delfino v. Agilent Technologies, Inc., 52 Ca.Rptr.3d 376 (Ca. Ct. App. 2006), the plaintiffs sued the employer of a man they claimed had sent them threatening emails and messages posted to online bulletin boards. The trial court granted the employer’s motion for summary judgment, and the plaintiffs appealed. The California Court of Appeals noted that no case had yet held that a corporate employer was a provider of an “interactive computer service” for providing internet access to its employees. Id. at 389. The court noted, however, that several commentators had indicated that an employer who provides its employees with internet access through the employer’s internal computer
system should be considered a provider of an interactive computer service for purposes of
the CDA. See id. (citing Zion, Protecting the E–Marketplace of Ideas by Protecting
Employers: Immunity for Employers Under Section 230 of the Communications Decency
(1999)). The California court also noted that “‘Internet resources and access are
sufficiently important to many corporations and other employers that those employers
link their office computer networks to the Internet and provide employees with direct or
modem access to the office network (and thus to the Internet).’” Id. (quoting Am. Civil
(1997)). The Delfino court ultimately concluded that the employer in that case met the
definition of a provider of an interactive computer service because “it ‘provide[d] or
enable[d] computer access by multiple users [i.e., Agilent’s employees] to a computer
server.’” Id. (quoting 47 U.S.C. § 230(f)(2)).

The Illinois Appellate Court came to a similar conclusion in Lansing v. Sw.
(Ill. 2012). In that case, the plaintiff sued the employer airline, claiming that it had
negligently supervised an employee who sent threatening messages. The trial court
granted summary judgment in favor of the airline, concluding that Section 230 of the
CDA afforded it immunity from the plaintiff’s claims that arose from the emails and text
messages sent over the internet. The plaintiff appealed and argued that the defendant was
an airline, not an ISP, and that when Congress enacted the CDA in 1996, it did not intend
to include within the definition of a provider of an interactive computer service those employers who gave their employees access to the Internet for the purpose of their work. Although the parties in Lansing focused their arguments on whether the airline was an ISP, the court observed that an ISP was neither mentioned nor defined by the CDA. Instead, the proper focus was on whether the airline was a provider of an interactive computer service. The court answered this question in the affirmative:

We find that, under the plain language of the statute and its broad definition of an ICS [interactive computer service], an employer like defendant qualifies as a provider or user of an ICS because defendant uses an information system or service that multiple users, like defendant’s employees, use to access the Internet.

Lansing, 980 N.E.2d at 637. Cf. Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d 772, 777 (Cal. Ct. App. 2001) (holding that public library was immune from suit under Section 230 because it provided an interactive computer service by enabling multiple users to access the internet through its public computers).

Here, the designated evidence clearly establishes that both 500 Festival and FedEx provide or enable computer access for multiple users on their respective computer networks to access the Internet by means of the servers on each network. We conclude that this is all that is required under Section 230(c)(1) to be considered a provider of an interactive computer service.

Of course, simply because the defendants here have established that they are providers of an interactive computer service does not mean that they are automatically immune from suits. Section 230 of the CDA does not provide blanket immunity for providers of an interactive computer service. Instead, it protects such providers only
from claims which seek to hold the provider as a “publisher.” Delfino, 52 Cal.Rptr.3d at 388; see also Craigslist, Inc., 519 F.3d at 669 (explaining that Section 230(c) “cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts.”). Instead, for a defendant to claim the protection afforded by Section 230 of the CDA, it must establish three elements: (1) that the defendant is a provider or user of an interactive computer service; (2) that the cause of action treats the defendant as a publisher or speaker of information; and (3) that the information at issue is provided by another information content provider. Delfino, 52 Cal.Rptr.3d at 388 (citing Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 714 (Cal. Ct. App. 2002)).

We have already concluded that both 500 Festival and FedEx are providers of an interactive computer service. And it is clear that the information at issue—the comments posted to the IBJ website—was provided by another “information content provider,” which is defined as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet[.]” 47 U.S.C. § 230(f)(3). FedEx’s unknown user and 500 Festival’s known employee, Wilson, easily fall within this definition.

The final question then is whether the Millers’ cause of action treats the defendants as publishers of the information. The Millers’ complaint clearly seeks to hold 500 Festival and FedEx liable for what they published. See Appellant’s App. p. 87 (“Mr. Wilson, 500 Festival, Ms. Hanlon, Mr. Leagre, Ms. Leagre, FedEx, Does #1-3, Mr. Burk, Ms. Steege, Mr. Starr and Ms. Starr, individually and/or in a concerted action among some or all of the Defendants, published unfounded statements regarding misuse of funds
and other criminal and/or lewd acts on the IBJ website, the Indianapolis Star website and WRTV-6s website”); id. at 88 (same); id. at 89 (same). And despite their references to other doctrines, such as *respondeat superior*, the Millers’ actual complaint seeks to hold 500 Festival and FedEx liable as publishers of the statements. Thus, their claims are barred by Section 230(c) of the CDA. See *Delfino*, 52 Cal.Rptr.3d at 389; *Lansing*, 980 N.E.2d at 637 (both holding that employers were protected by Section 230(c)(1) from suits seeking to hold them liable for the actions of their employees while using the employers’ computer networks to access the internet). Accordingly, the trial court properly granted summary judgment in favor of 500 Festival and FedEx.

**Conclusion**

Although there may have remained a genuine issue of material fact concerning spoliation of evidence under state law, the trial court properly granted summary judgment in favor of 500 Festival and FedEx, finding each to be sued in their capacity as a publisher of the information at issue and concluding that, as such, these defendants were immune from the Millers’ claims under Section 230(c) of the federal Communications Decency Act because these defendants are providers of an interactive computer service.

Affirmed.

BAILEY, J., and BRADFORD, J., concur.
In this suit, a group of New York residents who advocate for increased democracy in China sue one of China’s largest companies, Baidu, Inc. (incorrectly named in the Complaint as “Baidu.com Inc.”). Plaintiffs contend that Baidu, which operates an Internet search engine akin to Google, unlawfully blocks from its search results here in the United States articles and other information concerning “the Democracy movement in China” and related topics. (Compl. (Docket No. 1) ¶ 14, 22). The case raises the question of whether the First Amendment protects as speech the results produced by an Internet search engine. The Court concludes that, at least in the circumstances presented here, it does. Accordingly, allowing Plaintiffs to sue Baidu for what are in essence editorial judgments about which political ideas to promote would run afoul of the First Amendment. Baidu’s motion for judgment on the pleadings pursuant to Rule 12(c) of the Federal Rules of Civil Procedure is therefore GRANTED, and the Complaint is dismissed.
BACKGROUND

The following facts, which are taken from the Complaint unless otherwise noted, are assumed to be true for purposes of this motion. See, e.g., Gonzalez v. Hasty, 651 F.3d 318, 321 (2d Cir. 2011). Baidu operates a Chinese search engine service called Baidu.com, through which it “offers multiple services to locate information, products and services using Chinese-language search terms, such as, search by Chinese phonetics, advanced search, snapshots, spell checker, stock quotes, news, images, video, weather, train and flight schedules and other local information.” (Compl. ¶ 13). As of 2010, Baidu purported to be “the third largest search engine service provider in the world and the largest in China, with an estimated more than 70% share of the Chinese-language market.” Baidu, Inc. v. Register.com, Inc., 760 F. Supp.2d 312, 314 (S.D.N.Y. 2010) (citing Baidu’s complaint).

Plaintiffs, self-described “promoters of democracy in China through their writings, publications and reporting of pro-democracy events,” allege that Baidu conspires to prevent “pro-democracy political speech” from appearing in its search-engine results here in the United States. (Compl. ¶¶ 7-8, 10-12, 14-16, 20). Specifically, Plaintiffs claim that Baidu censor[s] and block[s] from search engine results any article, publication, video, audio and any information in whatever format if its content deals with the Democracy movement in China or any of the following topics that are related to the Chinese Democracy movement: The June 4th Movement, The Jasmine Revolution, The Jasmine Movement; The China Democracy Party National Committee and the Tiananmen Square Incident or movement. (Compl. ¶ 22). Plaintiffs claim that Baidu engages in this “censorship” at the behest of the People’s Republic of China (“China”), which was named as a defendant in the Complaint but was never served and is no longer a party to the case. (Compl. ¶ 23; see Docket No. 55).

---

1 This case has been the subject of two prior opinions by the Court, see Jian Zhang v. Baidu.com Inc., 932 F. Supp. 2d 561 (S.D.N.Y. 2013); Jian Zhang v. Baidu.com Inc., 293 F.R.D. 508 (S.D.N.Y. 2013), familiarity with which is assumed.
Each Plaintiff has published — on the Internet — articles, video recordings, audio recordings, or other publications regarding the democracy movement in China. (Compl. ¶¶ 24-47). Although such publications appear in results returned by other search engines, such as Google and Bing, they do not appear in Baidu’s search results because Baidu deliberately blocks them. (Id.). On these bases, Plaintiffs bring eight claims: (1) conspiracy to violate their civil rights, pursuant to 42 U.S.C. § 1985; (2) violation of their civil rights on the basis of race, pursuant to 42 U.S.C. § 1981; (3) violation of their civil rights under color of state law, pursuant to 42 U.S.C. § 1983; (4-7) denial of their right to equal public accommodations, in violation of New York Civil Rights Law §§ 40 and 40-c, New York Executive Law § 296(2), and New York City Administrative Code § 8-107(4)(a); and (8) denial of the equal protection of the laws guaranteed by New York Constitution Article 1, § 11. (Compl. ¶¶ 48-70). Plaintiffs seek $16,000,000 in damages, plus attorney’s fees and costs. (Compl. ¶¶ 71-72).2

LEGAL STANDARD

The standard of review for a motion for judgment on the pleadings under Rule 12(c) of the Federal Rules of Civil Procedure is the same as that governing motions to dismiss under Rule 12(b)(6). See, e.g., Patel v. Contemporary Classics of Beverly Hills, 259 F.3d 123, 126 (2d Cir. 2001). A plaintiff must plead facts sufficient “to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). In applying this standard, a court must assume all of the plaintiff’s “factual allegations to be true and draw[] all reasonable inferences in the plaintiff’s favor.” Harris v. Mills, 572 F.3d 66, 71 (2d Cir. 2009).

2 Although somewhat unclear, the Complaint also suggests that Plaintiffs seek unspecified “declaratory and injunctive relief.” (Compl. ¶ 4; see also Compl. ¶ 2. But see Compl. ¶ 72.)
DISCUSSION


Although the Supreme Court has not addressed the precise question at issue, its First Amendment jurisprudence all but compels the conclusion that Plaintiffs’ suit must be dismissed. The starting point for analysis is *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241, 258 (1974), in which the Court held that a Florida statute requiring newspapers to provide political candidates with a right of reply to editorials critical of them violated the First Amendment.

---

3 Curiously, Baidu cites neither these decisions nor the scholarship referenced above.
“Although the statute did not censor speech in the traditional sense — it only required newspapers to grant access to the messages of others,” the Court “found that it imposed an impermissible content-based burden on newspaper speech.” *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 653 (1994). The Court noted that, “in practical effect, Florida’s right-of-reply statute would deter newspapers from speaking in unfavorable terms about political candidates” and that it also “induced the newspaper to respond to the candidates’ replies when it might have preferred to remain silent.” *Id.* at 654. In both respects, the statute impermissibly infringed the newspaper’s First Amendment right to exercise “editorial control and judgment.” *Tornillo*, 418 U.S. at 258.

The Court later reinforced that principle, and extended it well beyond the newspaper context, in *Hurley v. Irish-American Gay, Lesbian, & Bisexual Group of Boston*, 515 U.S. 557 (1995). The question in *Hurley* was whether Massachusetts could “require private citizens who organize a parade to include among the marchers a group imparting a message the organizers do not wish to convey.” *Id.* at 559. The Court held that allowing the state to do so would “violate[] the fundamental rule of protection under the First Amendment, that a speaker has the autonomy to choose the content of his own message.” *Id.* at 573; see also, e.g., *Pac. Gas & Elec. Co. v. Pub. Util. Comm’n of Cal.*, 475 U.S. 1 (1986) (plurality opinion) (relying on *Tornillo* to invalidate a rule requiring a privately owned utility to include with its bills an editorial newsletter published by a consumer group critical of the utility’s ratemaking practices). “‘Since all speech inherently involves choices of what to say and what to leave unsaid,’” the Court explained, “‘one important manifestation of the principle of free speech is that one who chooses to speak may also decide ‘what not to say.’” *Hurley*, 515 U.S. at 573 (quoting *Pac. Gas & Elec. Co.*, 475 U.S. at 11, 16 (plurality opinion)). Notably, the Court found that principle applied even though the
parade organizers did not themselves create the floats and other displays that formed the parade and were “rather lenient in admitting participants.” *Id.* at 569. “[A] private speaker,” the Court stated, “does not forfeit constitutional protection simply by combining multifarious voices, or by failing to edit their themes to isolate an exact message as the exclusive subject matter of the speech. Nor . . . does First Amendment protection require a speaker to generate, as an original matter, each item featured in the communication.” *Id.* at 569-70.

Taken together, those decisions establish several principles relevant to this case. First, as a general matter, the Government may not interfere with the editorial judgments of private speakers on issues of public concern — that is, it may not tell a private speaker what to include or not to include in speech about matters of public concern. *See also* Snyder v. Phelps, 131 S. Ct. 1207, 1215 (2011) (“[S]peech on public issues occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection.” (internal quotation marks omitted)). Second, that rule is not “restricted to the press, being enjoyed by business corporations generally and by ordinary people engaged in unsophisticated expression as well as by professional publishers.” *Hurley*, 515 U.S. at 574. Third, the First Amendment’s protections apply whether or not a speaker articulates, or even has, a coherent or precise message, and whether or not the speaker generated the underlying content in the first place. *See generally* Zalewska v. Cnty. of Sullivan, *N.Y.*, 316 F.3d 314, 319 (“To be sufficiently imbued with communicative elements [to warrant protection under the First Amendment], an activity need not necessarily embody a narrow, succinctly articulate message, but the reviewing court must find, at the very least, an intent to convey a particularized message along with a great likelihood that the message will be understood by those viewing it.” (internal quotation marks omitted)). And finally, it does not matter if the Government’s intentions are noble — for example, to promote “press
responsibility,” *Tornillo*, 418 U.S. at 256, or to prevent expression that is “misguided, or even hurtful,” *Hurley*, 515 U.S. at 574; *see also Turner*, 512 U.S. at 640 (“[T]he mere assertion of dysfunction or failure in a speech market, without more, is not sufficient to shield a speech regulation from the First Amendment standards . . . .”). Put simply, “[d]isapproval of a private speaker’s statement”—no matter how justified disapproval may be—“does not legitimize use of the [Government’s] power to compel the speaker to alter the message by including one more acceptable to others.” *Hurley*, 515 U.S. at 581.

In light of those principles, there is a strong argument to be made that the First Amendment fully immunizes search-engine results from most, if not all, kinds of civil liability and government regulation. *See, e.g.*, Benjamin, *supra*, at 1458-72; Volokh & Falk, *supra*, at 884-92. The central purpose of a search engine is to retrieve relevant information from the vast universe of data on the Internet and to organize it in a way that would be most helpful to the searcher. In doing so, search engines inevitably make editorial judgments about what information (or kinds of information) to include in the results and how and where to display that information (for example, on the first page of the search results or later). *See generally* Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 Yale J.L. & Tech. 188, 192 (2006) (concluding that “search engines make editorial judgments just like any other media company”). In these respects, a “search engine’s editorial judgment is much like many other familiar editorial judgments,” such as the newspaper editor’s judgment of which wire-service stories to run and where to place them in the newspaper, the guidebook writer’s judgments about which attractions to mention and how to display them, and Matt Drudge’s judgments about which stories to link and how prominently to feature them. Volokh & Falk, *supra*, at 884; accord Benjamin, *supra*, at 1467-71.
On that theory of the First Amendment’s protection of search-engine results, the fact that search engines often collect and communicate facts, as opposed to opinions, does not alter the analysis. As the Supreme Court has held, “the creation and dissemination of information are speech within the meaning of the First Amendment. Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs.” *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011); see also Volokh & Falk, *supra*, at 889-90 (noting that the First Amendment “protects the collection and communication of facts as much as it protects opinions, including facts that are not ideologically laden — such as names of crime victims in three-sentence crime reports, names of accused juvenile offenders, lists of bestselling books, lists of tenants who had been evicted by local landlords, information in a mushroom encyclopedia, recipes in a cookbook, and computer program source code” (citing cases)). Nor does the fact that search-engine results may be produced algorithmically matter for the analysis. After all, the algorithms themselves were written by human beings, and they “inherently incorporate the search engine company engineers’ judgments about what material users are most likely to find responsive to their queries.” Volokh & Falk, *supra*, at 884; *see also id.* at 888-90; Benjamin, *supra*, at 1470. In short, one could forcefully argue that “what is true for parades and newspaper op-ed pages is at least as true for search engine output. When search engines select and arrange others’ materials, and add the all-important ordering that causes some materials to be displayed first and others last, they are engaging in fully protected First Amendment expression — ‘[t]he presentation of an edited compilation of speech generated by other persons.’” Volokh & Falk, *supra*, at 891 (quoting *Hurley*, 515 U.S. at 570).

In contrast to that robust theory of the First Amendment in this context, some scholars have relied on the Supreme Court’s decision in *Turner* — which Plaintiffs here do not cite — to
advocate for a lower level of protection of search-engine results. *See, e.g.*, Bracha & Pasquale, *supra*, at 1191-94. In *Turner*, the Court reviewed regulations requiring cable operators to carry the signals of a specified number of local broadcast television stations, and applied only intermediate scrutiny. *See* 512 U.S. at 662. Significantly, the Court began its analysis by stating that “[t]here can be no disagreement on an initial premise”: that cable operators, “by exercising editorial discretion over which stations or programs to include in its repertoire” — that is, by exercising editorial discretion over speech created by others — themselves “engage in and transmit speech” protected by the First Amendment. *Id.* at 636 (internal quotation marks omitted). Nevertheless, the Court held that an intermediate level of scrutiny was appropriate for several reasons: first, because cable operators were mere “conduit[s] for the speech of others, transmitting it on a continuous and unedited basis to subscribers,” *id.* at 629; *see id.* at 654-55; second, because cable operators had the ability to shut out some speakers, “giv[ing] rise to the Government’s interest in limiting monopolistic autonomy in order to allow for the survival of broadcasters who might otherwise be silenced and consequently destroyed,” *Hurley*, 515 U.S. at 577; and third, because the regulations at issue were content-neutral, as they did not “impose[] a restriction, penalty, or burden by reason of the views, programs, or stations the cable operator has selected or will select,” *Turner*, 512 U.S. at 644. That is, although acknowledging that the cable operators were engaged in speech, the Court granted lesser protection to that speech because of its less expressive nature, the technological quasi-monopoly in the marketplace of ideas enjoyed by the cable companies, and the fact that the regulations did not discriminate on the basis of content. Taking these rationales as lodestars, some scholars argue that search-engine results should also be afforded lesser protection under the First Amendment.
This Court, however, need not resolve the scholarly debate in order to decide the present motion because, whether or not the First Amendment shields all search engines from lawsuits based on the content of their search results, it plainly shields Baidu from Plaintiffs’ claims in this lawsuit. Here, the very theory of Plaintiffs’ claims is that Baidu exercises editorial control over its search results on certain political topics — namely, by disfavoring expression concerning “the Democracy movement in China” and related subjects. (Compl. ¶ 22). In other words, Plaintiffs do not — and, in light of their own allegations, cannot — make any argument that Baidu is merely an “infrastructure or platform that delivers content” in a neutral way. Bracha & Pasquale, supra, at 1192-97 (arguing that because “search engines do not function as publishers or editors of the content to which they channel users,” their results should not be treated as speech covered by the First Amendment). Instead, they seek to hold Baidu liable for, and thus punish Baidu for, a conscious decision to design its search-engine algorithms to favor certain expression on core political subjects over other expression on those same political subjects. To allow such a

---

4 Given the allegations in this case, there is also no need to address whether laws of general applicability, such as antitrust laws, can be applied to search engines without implicating the First Amendment. Compare Benjamin, supra, at 1482, 1487-92, with Volokh & Falk, supra, at 895-99. Nor is there any need to address whether a search engine could be held liable for false statements concerning its methodology or search results. Cf., e.g., Connecticut v. Moody’s Corp., No. X04HHDCV106008836S, 2012 WL 2149408, at *9 (Conn. Super. Ct. May 10, 2012) (holding that a state civil-enforcement action against a bond-rating agency for false statements about the manner in which the agency operated its business was not barred by the First Amendment even if the underlying ratings themselves enjoyed First Amendment protection).

5 As discussed below, whether any search engine is — or can be — the neutral conduit of information that Bracha and Pasquale describe is open to question, see, e.g., Benjamin, supra, at 1469-70, 1485-86; Volokh & Falk, supra, at 898-99, but it need not be addressed here.

6 That Plaintiffs allege that Baidu exercises editorial judgment “in cooperation with and according to the policies and regulations of” China makes no difference to the analysis. (Compl. ¶ 14). Plaintiffs allege that Baidu “purposely designs its systems and search engines to exclude” specific content. (Compl. ¶ 16). Whether it does so at the behest, or in furtherance of the interests, of China does not bear on the nature or extent of Baidu’s First Amendment rights.
suit to proceed would plainly “violate[] the fundamental rule of protection under the First Amendment, that a speaker has the autonomy to choose the content of his own message.” *Hurley*, 515 U.S. at 573; *see also, e.g.*, *Agency for Int’l Dev. v. Alliance for Open Soc’y Int’l*, 133 S. Ct. 2321, 2327 (2013) (“[F]reedom of speech prohibits the government from telling people what they must say.” (internal quotation marks omitted)).

That conclusion is compelled as much by *Turner* as it is by *Tornillo* and *Hurley*. First, in light of *Turner*, “[t]here can be no disagreement” that Baidu is “engage[d] in and transmit[s] speech” and is thus “entitled to the protection of the speech and press provisions of the First Amendment” because Plaintiffs’ own theory is that the company “exercise[s] editorial discretion” over its search results and thereby “seek[s] to communicate messages on a wide variety of topics and in a wide variety of formats.” 512 U.S. at 636 (internal quotation marks and alterations omitted). Second, *Turner*’s three principal rationales for applying a lower level of scrutiny to the must-carry cable regulations — namely, that cable companies were mere conduits for the speech of others, that they had the physical ability to silence other speakers, and that the regulations at issue were content-neutral — are inapplicable here. With respect to the first rationale, it is debatable whether any search engine is a mere “conduit” given the judgments involved in designing algorithms to choose, rank, and sort search results. *See, e.g.*, Benjamin, *supra*, at 1469-70, 1485-86; Volokh & Falk, *supra*, at 898-99. But whether or not that proposition is true as a general matter, it is plainly “not apt here,” as Plaintiffs’ own allegations of censorship make clear that Baidu is “‘more than a passive receptacle or conduit for news, comment, and advertising.’” *Hurley*, 515 U.S. at 575 (quoting *Tornillo*, 418 U.S. at 258). As Plaintiffs themselves allege, for example, Baidu “purposely designs its search engine algorithms
to exclude any pro-democracy topics, articles, publications, and multimedia coverage.” (Compl. ¶ 20).

The second rationale, too, has no application here, as search engine operators (at least in the United States and given today’s technology) lack the physical power to silence anyone’s voices, no matter what their alleged market shares may be. See Volokh & Falk, supra, at 897-98. As Plaintiffs’ own publications make clear (Compl. ¶¶ 24-47), Baidu does not have the ability to block “pro-democracy” writings from appearing on the Internet in this country altogether; it can only control whether it will help users find them. And if a user is dissatisfied with Baidu’s search results, he or she “has access, with just a click of the mouse, to Google, Microsoft’s Bing, Yahoo! Search, and other general-purpose search engines, as well as to almost limitless other means of finding content on the Internet, including specialized search engines, social networks, and mobile apps.” Volokh & Falk, supra, at 898. In fact, Plaintiffs themselves acknowledge that their pro-democracy works are widely available to the public on the Internet “via any of the well known [sic] search engines such as Google, Yahoo[,] and Bing.” (Compl. ¶ 24; see also Compl. ¶¶ 27, 30, 32, 36, 39, 42, 46).

It is, however, Turner’s third rationale for applying intermediate scrutiny that puts the final nail in the coffin for Plaintiffs’ claims in this case. In Turner, the Court concluded that the regulations at issue were content-neutral, as they did not “impose[] a restriction, penalty, or burden by reason of the views, programs, or stations the cable operator has selected or will select.” 512 U.S. at 644. By contrast, although the present case does not involve government regulation per se, Plaintiffs call upon the Court to impose a penalty on Baidu precisely because of what it does and does not choose to say. See id. at 643 (stating that government regulation that “by [its] terms “distinguish[es] favored speech from disfavored speech on the basis of the
ideas or views expressed [is] content based”). As the Turner Court made clear, however, “the First Amendment, subject only to narrow and well-understood exceptions” — inapplicable here — “does not countenance governmental control over the content of messages expressed by private individuals.” Id. at 641. Accordingly, to allow Plaintiffs’ suit to proceed, let alone to hold Baidu liable for its editorial judgments, would contravene the principle upon which “[o]ur political system and cultural life rest”: “that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence.” Id. at 641.

Plaintiffs’ arguments to the contrary are wholly unpersuasive. First, Plaintiffs assert — without citation to any legal authority — that “Baidu is not speaking,” but rather “engaging in discriminatory conduct” for which it can be held liable under federal civil rights laws and New York State’s public accommodations law. (Aff. Opp’n (Docket No. 50) (“Pls.’ Mem.”) ¶ 10). That assertion, however, is belied by Plaintiffs’ own theory of the case, which is that by exercising editorial discretion, Baidu favors some “political speech” over other “political speech.” (Compl. ¶ 11). See Turner, 512 U.S. at 636 (holding that cable operators are entitled to the protection of the First Amendment because, “by exercising editorial discretion over which stations or programs to include in [their] repertoire” — that is, by exercising editorial discretion over the speech of others — they “seek to communicate messages”) (internal quotation marks and alterations omitted); see also, e.g., Hurley, 515 U.S. at 569 (“[A] narrow, succinctly articulable message is not a condition of constitutional protection, which if confined to expressions conveying a particularized message would never reach the unquestionably shielded painting of Jackson Pollock, music of Arnold Schöenberg, or Jabberwocky verse of Lewis Carroll.”) (internal quotation marks and citation omitted)). Further, Plaintiffs’ argument is indistinguishable from the argument rejected in Hurley, that the parade at issue was a public
accommodation subject to Massachusetts’ own public accommodations law. That is, “once the expressive character” of Baidu’s search results “is understood, it becomes apparent” that allowing Plaintiffs to sue Baidu based on the content of those results would have “the effect of declaring [Baidu’s] speech itself to be the public accommodation.” 515 U.S. at 572-73.

Second, Plaintiffs argue that, even if Baidu’s search results are a form of speech, the First Amendment is not implicated because this is a private suit and thus does not involve direct government regulation. (Pls.’ Mem. ¶ 12). But that argument is also flatly inconsistent with Hurley, which was likewise a private suit in which the plaintiffs relied on a state public accommodations law. Moreover, the Supreme Court has long made clear that the First Amendment’s protections extend to private suits for money damages based on the content of speech. See, e.g., N.Y. Times Co. v. Sullivan, 376 U.S. 254, 277-78 (1964) (holding that “[w]hat a State may not constitutionally bring about by means of a criminal statute is likewise beyond the reach of its civil law of libel,” and noting that the “the pall of fear and timidity” that the threat of civil liability would impose upon those who would speak “is an atmosphere in which the First Amendment freedoms cannot survive”); see also, e.g., Dongguk Univ. v. Yale Univ., 734 F.3d 113, 129 (2d Cir. 2013) (holding that “heightened First Amendment protections apply to any tort alleging reputational harm as long as the underlying speech relates to a matter of public concern”). The bottom line is that Plaintiffs seek to enlist the government — through the exercise of this Court’s powers — to impose “a penalty on the basis of the content” of Baidu’s speech. Tornillo, 418 U.S. at 256. To allow it to do so would “inescapably ‘dampen[] the vigor and limits the variety of public debate.’” Id. at 257 (quoting N.Y. Times Co., 376 U.S. at 279); see also Langdon, 474 F. Supp. 2d at 629-30 (dismissing First Amendment, fraud, and deceptive
business practices claims against a search engine as barred by the First Amendment); Search King, 2003 WL 21464568, at *4 (same with respect to a tortious-interference claim).

Third, Plaintiffs contend that Baidu’s search results, if speech, are a form of commercial speech subject to “relaxed” scrutiny under the First Amendment. (Pls.’ Mem. ¶¶ 9-10). “The search engine,” Plaintiffs reason, “is both Baidu’s product and advertisement. There are no membership requirements and no usage fees because Baidu makes money selling advertisements and sponsorships. Thus, Baidu has a profit motive to retrieve and disseminate information on its search engine, for example, by drawing traffic to its site to sell advertisement [sic].” (Id. ¶ 10). Commercial speech, however, is defined as “expression related solely to the economic interests of the speaker and its audience.” Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y., 447 U.S. 557, 561 (1980) (emphasis added); see also United States v. United Foods, Inc., 533 U.S. 405, 409 (2001) (stating that commercial speech is “usually defined as speech that does no more than propose a commercial transaction”). That definition would presumably apply to advertisements displayed by a search engine, and might even apply to “search results shown to purposefully advance an internal commercial interest of the search provider.” Ballanco, supra, at 90 (arguing that such results “should be classified as commercial speech and, therefore, subject to less First Amendment protection”); see also Volokh & Falk, supra, at 885 (implicitly acknowledging that paid advertisements may be entitled to less protection under the First Amendment than “search results for which no payment has been made”). But that definition plainly does not apply to the search results at issue in this case, which relate to matters of public concern and do not themselves propose transactions. And, of course, the fact that Baidu has a
“profit motive” does not deprive it of the right to free speech any more than the profit motives of the newspapers in *Tornillo* and *New York Times* did.⁷

In short, Plaintiffs’ efforts to hold Baidu accountable in a court of law for its editorial judgments about what political ideas to promote cannot be squared with the First Amendment. There is no irony in holding that Baidu’s alleged decision to disfavor speech concerning democracy is itself protected by the democratic ideal of free speech. As the Supreme Court has explained, “[t]he First Amendment does not guarantee that . . . concepts virtually sacred to our Nation as a whole . . . will go unquestioned in the marketplace of ideas.” *Texas v. Johnson*, 491 U.S. 397, 418 (1989). For that reason, the First Amendment protects Baidu’s right to advocate for systems of government other than democracy (in China or elsewhere) just as surely as it protects Plaintiffs’ rights to advocate for democracy. Indeed, “[i]f there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable.” *Id.* at 414 (citing cases). Thus, the Court’s decision — that Baidu’s choice not to feature “pro-democracy political speech” is protected by the First Amendment — is itself “a reaffirmation of the principles of freedom and inclusiveness that [democracy] best reflects, and of the conviction that our toleration of criticism . . . is a sign and source of our strength.” *Id.* at 419.

**CONCLUSION**

For the foregoing reasons, Defendants’ motion for judgment on the pleadings is GRANTED, and the Complaint is dismissed in its entirety.⁸ Further, as any amendment would

---

⁷ Even if the speech in this case did qualify as “commercial speech,” it is far from clear that Plaintiffs’ claims would be consistent with the First Amendment. *See Cent. Hudson*, 447 U.S. at 556 (establishing a four-part test to determine whether a commercial-speech regulation is consistent with the First Amendment). The Court need not address that question.

⁸ Because the Court grants Baidu’s motion on First Amendment grounds, it need not and
be futile, Plaintiffs’ request for leave to amend to address any deficiencies in their Complaint is
.denied. The Clerk of Court is directed to terminate Docket No. 46 and close the case.

SO ORDERED.

Dated: March 27, 2014
New York, New York

JESSE M. FURMAN
United States District Judge

J. Pleadings (Docket No. 47) 6-8).
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ENRICO MORETTI, an individual, on behalf of himself, the general public and those similarly situated,

Plaintiff,

v.

THE HERTZ CORPORATION; HERTZ GLOBAL HOLDINGS, INC.; DOLLAR THRIFTY AUTOMOTIVE GROUP INC.; HOTWIRE, INC.; and DOES 1 THROUGH 25,

Defendants.

ORDER GRANTING MOTION TO TRANSFER

Now before the Court is the motion to transfer pursuant to 28 U.S.C. § 1404(a) filed by Defendants Hertz Corporation and Hertz Global Holdings Inc. (“Hertz”), Dollar Thrifty Automotive Group (“Dollar”), and Hotwire Inc. (“Hotwire”) (collectively “Defendants”). Having carefully reviewed the parties’ papers, relevant legal authority, the record in this case, and considered their arguments, the Court hereby GRANTS Defendants’ motion to transfer.

BACKGROUND

Plaintiff, Enrico Moretti (“Plaintiff”) filed a Complaint (“Complaint”) with four causes of action for violations of: (1) California Business and Professions Code Section 17500; (2) California Civil Code Section 1750; (3) state common and statutory law for fraud, deceit and misrepresentation; and (4) California Business and Professions Code Section 17200. According to the allegations in the Complaint, which must be taken as true at this procedural posture,
Defendants advertised a low rental car rate then actually charged Plaintiff a higher rental car rate in Mexico, failed to disclose that insurance purchase is mandatory at the time of rental, and inflated exchange rates at the time of payment. (See Compl. ¶¶ 26, 31, 34.) Plaintiff resided in California during the alleged incident and all the Defendants were Delaware corporations with principal places of business in New Jersey (Hertz), Oklahoma (Dollar) and California (Hotwire). (Id. at ¶¶ 4-8.)

“On December 15, 2012, Plaintiff reserved a [car rental from Hertz and Dollar] on the Hotwire website.” (Id. at ¶ 34.) “Hotwire specifically represented to Plaintiff that the fee for renting the selected car type . . . [was] an estimated total cost . . . of $365.23 for the ten-day rental, which included estimated taxes and fees” with a confirmation email to this effect. (Id. at ¶¶ 34, 36.) Neither Hotwire’s website nor the confirmation emails notified Plaintiff “that he would be required to purchase mandatory personal liability insurance from [Hertz and Dollar].” (Id.) Before completing his reservation on Hotwire, Plaintiff had to accept Hotwire’s Terms of Use (“Terms of Use”). (Declaration of Sarah Bernard (“Bernard Decl.”) ¶¶ 2-3; Declaration of Jacob Aaron Joachin Hadary (“Hadary Decl.”) ¶¶ 2-5.) On December 27, 2012, Plaintiff’s scheduled pickup day for his ten-day car rental in San Jose del Cabo Mexico, Hertz and Dollar “converted Plaintiff’s daily rate . . . using [Hertz and Dollar] arbitrary currency exchange rate.” (Id. at ¶¶ 35, 37, 39.) On January 6, 2013, after Plaintiff returned his rental car to Hertz and Dollar the total cost charged to Plaintiff’s credit card totaled $683.59 “which included the daily rental fee for ten days, airport fees, insurance and tax.” (Id. at ¶ 39.) Plaintiff alleges this is a regular business practice for Defendants and similarly situated individuals have been routinely overcharged and misinformed. (Id. at ¶ 41.)

ANALYSIS

A. Applicable Legal Standard.

Defendants move to transfer this action to the District Court of Delaware. Pursuant to 28 U.S.C. Section 1404(a), a district court may transfer a civil action to any district where the case could have been filed originally for the convenience of the parties and witnesses and in the interest of justice. The moving party bears the burden of showing the inconvenience of litigating in this forum favors transfer. See Florens Container v. Cho Yang Shipping, 245 F. Supp. 2d 1086, 1088 (N.D. Cal. 2002) (citing Commodity Futures Trading Comm’n v. Savage, 611 F.2d 270, 279 (9th Cir. 1979)). Moreover, the moving party cannot rely on vague generalizations to show the requisite factors weigh in favor of transfer. See id. at 1093. A district court has broad discretion “to adjudicate motions for transfer according to an individualized, case-by-case consideration of convenience and fairness.” Stewart Org., Inc. v. Ricoh Corp., 487 U.S. 22, 29 (1988) (quoting Van Dusen v. Barrack, 376 U.S. 612, 622 (1964) (internal citations omitted)).

In order for a district court to transfer an action under Section 1404, the court must make the following two findings: (1) the transferee court is one where the action “might have been brought,” and (2) the convenience of the parties and witnesses and the interest of justice favor transfer. Hatch v. Reliance Ins. Co., 758 F.2d 409, 414 (9th Cir. 1985). To determine whether the moving party has met its burden under the second prong, the Court considers the following factors: non-moving party’s choice of forum; convenience of the parties and witnesses; ease of access to sources of proof; local interest in the controversy; familiarity of each forum with the applicable law; and relative congestion in each forum. Decker Coal Co. v. Commonwealth Edison Co., 805 F.2d 834, 843 (9th Cir. 1986) (citing Gulf Oil Corp. v. Gilbert, 330 U.S. 501, 508 (1947)).

However, if a motion for transfer is based on a forum-selection clause, the analysis is adjusted in three ways. Atl. Marine Const. Co., Inc. v. U.S. Dist. Court for W. Dist. of Texas, 134 S. Ct. 568, 581-82 (2013):

First, the plaintiff’s choice of forum merits no weight, and the [plaintiff] bears the burden of establishing that transfer to the forum for which the parties bargained is unwarranted. . . . Second . . . [the] court should not consider arguments about the parties’ private interests . . . [the] court [ ] must deem the private-interest factors to
weigh entirely in favor of the preselected forum . . . [and] may consider arguments about public-interest factors only. . . . Third, when a party bound by a forum-selection clause flouts its contractual obligation and files suit in a different forum, a § 1404(a) transfer of venue will not carry with it the original venue’s choice of law rules – a factor that in some circumstances may affect public-interest considerations. Id.

Before the Court engages in the adjusted Section 1404(a) analysis, the Court must first determine whether a valid forum-selection clause exists within the subject contract. See Chateau des Charmes Wines Ltd. v. Sabate USA Inc., 328 F.3d 528, 530 (9th Cir. 2003) Determining this contractual issue is a two-part inquiry: (1) if the parties agreed to the clause; and (2) if the clause applies to the issue in dispute. See id.

B. Motion to Transfer.

1. Forum Selection Clause.

   i. Validity of the Clause.

   Defendants move to transfer this action on the basis that Plaintiff agreed to the Terms of Use containing a forum-selection clause mandating that disputes be resolved in the District of Delaware. When deciding whether the parties agreed to a certain matter, “courts generally . . . should apply ordinary state-law principles that govern the formation of contracts.” First Options of Chicago, Inc. v. Kaplan, 514 U.S. 938, 944 (1995). Consent is an essential element of any contract, and must be free, mutual and communicated. See Cal. Civ. Code §§ 1550, 1565, 1580. “[T]he forum-selection clause is unenforceable as to any particular plaintiff if the court determines that such plaintiff did not have sufficient notice of the forum-selection clause prior to entering into the contract.” Carnival Cruise Lines, Inc. v. Superior Ct., 234 Cal. App. 3d 1019, 1026-27 (1991). “Absent such notice, the requisite mutual consent to that contractual term is lacking and no valid contract with respect to such clause thus exists.” Id. at 1027. “[T]he forum selection clause . . . in an adhesion contract is enforceable even though the [party] did not actually read it as long as the clause provided adequate notice to the defendant that he was agreeing to the jurisdiction cited in the contract.” Hunt v. Super. Ct., 81 Cal. App. 4th 901, 908 (2000) (internal citations omitted). A binding contract is created if a “[p]laintiff [i]s provided with an opportunity to review the terms of service in the form of a hyperlink immediately under the I accept’ button and [ ] admittedly clicked ‘Accept.’” Swift v. Zynga Game Network, Inc., 805 F. Supp. 2d 904, 912 (N.D. Cal. 2011) It is sufficient to “requir[e]
a user to affirmatively accept the terms, even if the terms are not presented on the same page as the acceptance button” as long as the user has “access to the terms of service.”

It is undisputed that Plaintiff used the Hotwire website on December 15, 2012 to book his car rental for Mexico. (See Compl. ¶ 34; Hadary Decl. ¶ 7.) Plaintiff argues that Defendants have not met their burden to demonstrate that he agreed to the forum-selection clause contained in the Terms of Use. Specifically, Plaintiff alleges that Hotwire may have made a false representation in his access to the Terms of Use and argues that perhaps the hyperlink was not functioning properly at the time Plaintiff made his purchase. (Opp. Br. at 9.) Defendants have produced two declarations from employees at Hotwire: (1) Sarah Bernard who at the operative time was the Vice President of Product Management for Hotwire; and (2) Jacob Aaron Joachin Hadary who was the Lead Product Manager for Hotwire during that time. (See Bernard Decl. ¶ 1; see Hadary Decl. ¶ 1.) Bernard and Hadary affirmatively state that the Terms of Use in operation during the December 2012 time frame included a forum-selection clause. (See Bernard Decl. ¶ 4; Hadary Decl. ¶ 8.) Hadary declares, and corroborates Bernard’s declaration, that an individual using the Hotwire website cannot complete a booking without checking the “Acceptance Box” acknowledging the acceptance of “Hotwire’s terms and conditions and other applicable rules.” (Hadary Decl. ¶¶ 2-3.) Hadary confirms that this requirement has been in place since 2005. (See id. at ¶ 4.) Plaintiff confirms that he completed his booking through the Hotwire website which indicates that he checked the Acceptance Box. (See id. at ¶ 7; see also Compl. ¶ 34.) The language in the Acceptance Box shows that even though the terms were provided by hyperlink Plaintiff acknowledged accepting the “terms of use and Hotwire’s” rules. (Hadary Decl. ¶ 5.) The Court concludes that, in the absence of an affirmative denial from Plaintiff that he did not in fact check the Acceptance Box and clear evidence that Plaintiff could have not otherwise completed his car reservation, Plaintiff had notice and consented

1 “The ‘clickwrap’ process [is used] to obtain a user’s consent to terms of service whereby the terms of service are presented on the screen and do not allow the user to proceed without clicking to assent to the terms.” Swift v. Zynga Game Network, Inc., 805 F. Supp. 2d 904, 910 (N.D. Cal. 2011). The ‘modified clickwrap’ process is where the terms of service are not visible on the page but instead are linked by [a] hyperlink [to a different page or area] following the ‘Allow’ button,” where the terms of service are presented. Id.

2 Under California Code of Civil Procedure Section 2015.5, declarations under penalty of perjury are a form of evidence allowed in support of a motion for transfer.
to the Terms of Use containing the forum-selection clause. (See Opp. Br. at 9.) The Court finds that
the parties agreed to the forum-selection clause contained in the December 2012 version Terms of Use and it is therefore valid.

ii. Scope of Clause - Dispute.

Second, having established that a valid forum-selection clause exists, the Court must now determine if the dispute at hand falls within the scope of forum-selection clause. “[T]he scope . . . of a forum selection clause is a matter of contract.” *Polar Shipping Ltd. v. Oriental Shipping Corp.*, 680 F.2d 627, 632 (9th Cir. 1982). “Where the plaintiff has agreed to bring suit in a specific forum, presumably in exchange for other promises from the defendant, the plaintiff has already exercised their privilege to select venue.” *Atl. Marine Constr.*, 134 S. Ct. at 582. “In agreeing to the clause, the parties waived their right to challenge the preselected forum as inconvenient or less convenient for themselves, or their witnesses, or for their pursuit of the litigation.” *Id.* “A forum selection clause is presumptively valid; the party seeking to avoid a forum selection clause bears a ‘heavy burden’ to establish a ground upon which we will conclude the clause is unenforceable.” *Doe 1 v. AOL LLC*, 552 F.3d 1077, 1083 (9th Cir. 2009) (citing *M/S Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1, 17 (1972)).

Here, the forum selection clause states that Plaintiff “consents to the exclusive jurisdiction and venue of the courts located in Delaware . . . for all disputes arising out of, or relating to, the Terms and Conditions and use of this site.” (Hertz and Dollar Motion, Ex. A.) In the Complaint Plaintiff alleges that “[t]his case arises out of Defendants’ false advertising of rental cars . . . applying undisclosed, inflated currency exchange rates to the cost of rentals.” (See Compl. ¶ 1.) Specifically, Plaintiff alleges that “Hotwire partners with rental service providers . . . to market, advertise and sell, via the Hotwire Website, car rental services.” (See *id.* at ¶ 23.) Additionally, the Terms of Use state that, “[t]o the extent that you book any travel products or services on this Site . . . you agree that these Terms and Conditions shall apply to all such transactions.” (Hertz and Dollar Motion, Ex. A.) This case arises out of the Terms of Use because Plaintiff booked a car rental for his travel to Mexico through Hotwire’s website and obtained the car rental from Hertz and Dollar, a rental service provider advertised on Hotwire’s website. (See
Compl. ¶ 34.) Therefore, this dispute is within the scope of the Terms of Use forum-selection clause.

iii. Scope of Clause - Third-Party Beneficiaries.

Hertz and Dollar move to transfer on the basis that they have standing to enforce the forum-selection clause in the Terms of Use. “[A] range of transaction participants, parties and non-parties, should benefit from and be subject to forum selection clauses.” Manetti-Farrow, Inc. v. Gucci Am., Inc., 858 F.2d 509, 514 n.5 (9th Cir. 1988) “A third-party qualifies as a beneficiary under a contract if the parties intended to benefit the third party and the terms of the contract make that intent evident.” Karo v. San Diego Symphony Orchestra Ass’n, 762 F.2d 819, 821-22 (9th Cir. 1985). “Although the beneficiary need not be named in the contract, he must be a member of a class referred to and identified in it.” Id. at 822. “In the Ninth Circuit, a third-party beneficiary of an agreement is bound by the terms of the agreement, including a valid forum selection clause.” eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1162 (N.D. Cal. 2009); see also TAAG Linhas Aereas de Angola v. Transamerica Airlines, Inc., 915 F.2d 1351, 1354 (9th Cir. 1990) (“it is well-settled contract law that the scope of a third-party beneficiary’s rights is defined by the contract . . . a forum selection clause can restrict a third-party beneficiary to the designated forum.”). Furthermore, if “the alleged conduct of the non-parties is so closely related to the contractual relationship [ ] the forum selection clause applies to all defendants.” Manetti-Farrow, Inc., 858 F.2d at 514 n.5.

It is undisputed that Hertz and Dollar are not signatories to the Terms of Use. (See Hertz and Dollar Motion at 8; see also Opp. Br. at 19.) However, Hertz and Dollar allege that they have standing to enforce the forum selection clause as third-party beneficiaries to the Terms of Use. (See Hertz and Dollar Motion at 9.) The Terms of Use indicate that the Hotwire website “offers products, services, advice, merchandise and information through [Providers] on an ‘as is,’ ‘as available’ basis.” (See id., Ex. A.) This provides that Providers be considered third-party beneficiaries to the Terms of Use. Hertz and Dollar fit into the class of Providers because Plaintiff claims that he booked his car rental on the Hotwire website and on December 27, 2012 he picked up his ten-day car rental at Hertz and Dollar’s Mexico location. (See Compl. ¶ 37.) After Plaintiff returned his car
rental on January 6, 2013, Hertz and Dollar charged his credit card $638.59 for the car rental service. (See id. at ¶ 39.) Additionally, the Terms of Use also state that “Hotwire . . . shall not be responsible for any Provider’s failure to comply with these Terms and Conditions.” (Hertz and Dollar Motion, Ex. A.) The parties to this contract intended the Terms of Use to bind Hertz and Dollar by explicitly stating an expectation of compliance by all parties, including providers. Therefore, Hertz and Dollar are third-party beneficiaries with standing to enforce the forum-selection clause in the Terms of Use. Consequently, the Court does not address Hertz and Dollar’s alternate contention that they also have standing to enforce the forum selection clause as non-parties to the Terms of Use. (See Hertz and Dollar Motion at 9.)

In sum, the Court finds that the forum selection clause in the Terms of Use is valid and enforceable.

2. Public Interest Factors.

Defendants move to transfer on the grounds that this case does not present public interest factors in favor of retaining the case in this Court. Public interest “factors will rarely defeat a transfer motion, the practical result is that forum-selection clauses should control except in unusual cases.” Atl. Marine Constr., 134 S. Ct. at 582. “Public-interest factors may include ‘the administrative difficulties flowing from court congestion; the local interest in having localized controversies decided at home; [and] the interest in having the trial of a diversity case in a forum that is at home with the law.’” Id. at 581 n.6 (quoting Piper Aircraft Co. v. Reyno, 454 U.S. 235, 241, n.6 (1981) (internal quotation marks omitted)). Because this is not strictly a diversity case, the third factor is not applicable here.³ Therefore, the Court will examine the first two factors to determine whether the Plaintiff demonstrates that the “public interest factors overwhelmingly disfavor transfer.” Id. at 583.

³ This action was removed from state court to this Court on the basis of federal jurisdiction pursuant to the Class Action Fairness Act. (See Docket No. 1.) Therefore, the Court will discuss the choice-of-law issue, one closely related to this third factor, under section 3.
i. Court Administrative Difficulties.

Defendants contend that there are no known administrative difficulties flowing from court congestion which would favor this Court over the court in Delaware. “Administrative difficulties follow for courts when litigation is piled up in congested centers instead of being handled at its origin.” *Gulf Oil Corp.*, 330 U.S. at 508. In a transfer determination, it is important for the court to consider pendency of another action where consolidation of discovery, convenience of witnesses and parties may have positive effects in case administration. *A. J. Indus., Inc. v. U.S. Dist. Ct. for Cent. Dist. of Cal.*, 503 F.2d 384, 389 (9th Cir. 1974). “To permit a situation in which two cases involving precisely the same issues are simultaneously pending in different District Courts leads to the wastefulness of time, energy and money that § 1404(a) was designed to prevent.” *Cont’l Grain Co. v. The FBL-585*, 364 U.S. 19, 26 (1960).

Here, Plaintiff filed this action in the same District as a similar case, *Shahar v. Hotwire Inc, et al*, Case No. C 12-06027 JSW. On March 13, 2014, Defendants notified the Court that the parties in *Shahar* have signed a stipulation of settlement pending preliminary approval from this Court. (See Docket No. 51.) Defendants state that the stipulated settlement involves a class that does not include Plaintiff or any other classes Plaintiff attempts to represent in this matter. (See id.) At this juncture, although this action and *Shahar* are related cases, the two matters are in distinctly dissimilar procedural postures. The Court finds that the judicial economy factor does not weigh in favor of maintaining this action in this District in the face of pending settlement in a related matter.

ii. Local Interest in the Litigation.

Defendant moves to transfer on the grounds that because Plaintiff seeks to represent a class of similarly situated persons within the United States, this is not a controversy localized to California. “The local interest factor . . . determin[es] if the forum in which the lawsuit was filed has its own identifiable interest in the litigation which can justify proceeding in spite of these burdens.” *Carijano v. Occidental Petroleum Corp.*, 643 F.3d 1216, 1232 (9th Cir. 2011). “[W]ith this interest factor, we [do not] ask . . . whether another forum also has an interest.” *Tuazon v. R.J.*
Reynolds Tobacco Co., 433 F.3d 1163, 1182 (9th Cir. 2006). When “defendants are not California corporations, California has little interest in keeping the litigation in this state to deter future wrongful conduct.” Guimei v. Gen. Elec. Co., 172 Cal. App. 4th 689, 703 (2009) “[T]he local interest factor weighs in favor of a California forum where a California plaintiff is suing a California defendant over conduct that took place in the state.” Carijano, 643 F.3d at 1233. A state has personal jurisdiction over a defendant corporation if the corporation is incorporated or has its principal place of business within that state’s borders. J. McIntyre Mach., Ltd. v. Nicastro, 131 S. Ct. 2780, 2787 (2011).

In this case, there is a California plaintiff, possibly a California defendant, but no proof that the conduct took place in California. Plaintiff made his reservation on the Hotwire website, at which time he was a resident of California. (Compl. ¶¶ 4, 34.) All the Defendants are Delaware corporations with principal places of business in New Jersey (Hertz), Oklahoma (Dollar) and California (Hotwire). (Id. at ¶¶ 5-8.) Only Hotwire has their principal place of business in California. (See id. at ¶¶ 4, 8.) California may have an identifiable interest in protecting Plaintiff and in regulating Hotwire’s business activity within its boundaries. See Carijano, 643 F.3d at 1232. Although Hotwire’s residency weighs slightly in favor of California’s interest, this is counterbalanced by the fact that Hotwire is also a Delaware resident just like the other two defendants. In addition, Plaintiff does not allege that any of the false advertising activities took place in California, but only alleges that Defendants’ activities affect the State of California. (See id. at ¶¶ 17-18, 34, 36.) The lack of evidence that any of the alleged activities actually took place in California weighs against California’s interest in regulating Defendants’ future business activity within its borders. See Carijano, 643 F.3d at 1233. Therefore the local interest factor does not favor this forum.

This Court concludes that the public interest factors do not outweigh the parties’ contractual interests in designating Delaware as the preferred forum for dispute resolution. See Atl. Marine

---

4 Because this factor does not require the Court to evaluate the interest of another forum, this Court does not address Plaintiff’s contention regarding Delaware’s lack of interest in this litigation. (See Opp. Br. at 19.)
Const. Co., Inc., 134 S.Ct. at 583. The Court finds that the public interest factors do not favor maintaining this action in this District.

3. **Choice of Law Rules.**

The parties dispute whether the District of Delaware has the appropriate expertise to handle this matter because it may involve California law. Defendant argues that district courts regularly apply state law from different jurisdictions, when a case such as this involves both federal and state law. There is an exception under a Section 1404(a) to the rule barring a carrying over of the original forum’s law to the transferee district. *See id.* at 582. The Supreme Court “deemed that exception necessary to prevent ‘defendants, properly subjected to suit in the transferor State,’ from ‘invok[ing] § 1404(a) to gain the benefits of the laws of another jurisdiction.’” *Id.* (quoting *Van Dusen v. Barrack*, 376 U.S. 612, 638 (1964)). “[A] plaintiff who files suit in violation of a forum-selection clause enjoys no such ‘privilege’ with respect to its choice of forum, and therefore it is entitled to no concomitant ‘state-law advantages.’” *Id.* at 583. It would “be inequitable to allow the plaintiff to fasten its choice of substantive law to the venue transfer.” *Id.* The transferee court should “not apply the *Van Dusen* rule when a transfer stems from enforcement of a forum-selection clause” because “the parties waived their right” to enforce other state laws besides those named in the forum-selection clause. *Id.* However, it is against public policy for a defendant to include a choice of law provision in order “to insulate itself from liability against all statutory [based] claims, except perhaps those brought by Delaware residents.” *Millett v. Truelink, Inc.*, 2006 WL 2583100, at *4 (D. Del. Sept. 7, 2006). In such a case, the Delaware Court allowed the claims to proceed under *Plaintiff’s chosen forum state’s law.* *Id.*

Here, all of *Plaintiff’s* causes of action arise out of California law. Plaintiff admits that California law governs this action despite the choice-of-law rule mandating Delaware law. (*See Opp. Br. at 18; see Hertz and Dollar Motion at Ex. A.*) Plaintiff further argues that because all the claims are based on California law it is in the public’s interest for this action to remain in the “forum that is at home with the law.” *Atl. Marine Constr.*, 134 S. Ct. at 581 n.6. This action was removed from state court to this Court on the basis of the Class Action Fairness Act. (*See Docket No. 1.*)
Although this Court may be more familiar with the relevant law, there is nothing to indicate that the District of Delaware cannot adequately apply California law.

CONCLUSION

For the reasons stated herein, Defendants’ motion to transfer is GRANTED. The Clerk shall close this file and transfer this action to the District Court of Delaware forthwith.

IT IS SO ORDERED.

Dated: April 11, 2014

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE
Plaintiff Khalilah Wright ("Wright" or "Plaintiff") brings this putative class action against Defendant LinkedIn Corporation ("Defendant" or "LinkedIn"). Presently before the Court is LinkedIn’s Motion to Dismiss Plaintiff’s Second Amended Consolidated Complaint ("SAC"). The Court has fully reviewed the parties’ submissions and heard oral arguments of counsel presented at the hearing on November 22, 2013. For the reasons explained below, the Court has determined that LinkedIn’s Motion will be GRANTED IN PART and DENIED IN PART.
I. BACKGROUND

The following facts are taken from Plaintiff’s SAC. LinkedIn owns and operates the website www.LinkedIn.com, which provides an online community for professional networking.

Prospective members may sign up for a membership by providing a valid email address and registration password, which LinkedIn stores on its database. Once registered, a member may create a free online professional profile containing such information as employment and educational history.

When members register, they are required to confirm that they agree to LinkedIn’s User Agreement (“User Agreement”) and Privacy Policy (“Privacy Policy”). The Privacy Policy contains a statement that “[a]ll information that you provide will be protected with industry standard protocols and technology.”

For a monthly fee, members can upgrade to a paid “premium” subscription which grants them increased networking tools and capabilities. Members who purchase a premium subscription agree to the same terms and services of the User Agreement and Privacy Policy as if they were non-paying members.

Plaintiff alleges that sometime in 2012 hackers infiltrated LinkedIn’s computer systems and services. On June 6, 2012, the hackers posted approximately 6.5 million stolen LinkedIn users’ passwords on the Internet. On or around June 9, 2012, LinkedIn released a statement on its blog stating that it had recently completed a switch of its password encryption method from a system that stored member passwords in a hashed format to one that used both salted\(^1\) and hashed\(^2\) passwords for increased security.

Plaintiff alleges that she paid for a premium subscription from March 2010 until approximately August 2010. She alleges that her LinkedIn password was retrieved by the hackers and posted on the Internet on June 6, 2012. She alleges that, prior to her purchase of the premium subscription, she was not aware that her LinkedIn password was retrieved by the hackers.

---

\(^{1}\) According to the SAC, “salting” is an encryption process that protects information by concatenating a plaintext password with a series of randomly generated characters prior to hashing.

\(^{2}\) According to the SAC, “hashing” is an encryption process that protects information by applying a one-way function or algorithm to it. Hash functions are designed to reveal no information about the underlying input and are designed such that minor changes in inputs will result in major changes to outputs.
subscription, she read LinkedIn’s User Agreement and Privacy Policy and that, had LinkedIn disclosed its lax security practices, she would have viewed the premium subscription as less valuable and would either have attempted to purchase a premium subscription at a lower price or not at all.

II. LEGAL STANDARDS

a. Motion to dismiss under Rule 12(b)(1)

A Rule 12(b)(1) motion to dismiss tests whether a complaint alleges grounds for federal subject matter jurisdiction. If the plaintiff lacks standing under Article III of the U.S. Constitution, then the court lacks subject matter jurisdiction, and the case must be dismissed. See Steel Co. v. Citizens for a Better Env’t, 523 U.S. 83, 101-02 (1998).

A jurisdictional challenge may be facial or factual. Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). Where the attack is facial, the court determines whether the allegations contained in the complaint are sufficient on their face to invoke federal jurisdiction, accepting all material allegations in the complaint as true and construing them in favor of the party asserting jurisdiction. See Warth v. Seldin, 422 U.S. 490, 501 (1975). Where the attack is factual, however, “the court need not presume the truthfulness of the plaintiff’s allegations.” Safe Air for Everyone, 373 F.3d at 1039. In resolving a factual dispute as to the existence of subject matter jurisdiction, a court may review extrinsic evidence beyond the complaint without converting a motion to dismiss into one for summary judgment. See id.; McCarthy v. United States, 850 F.2d 558, 560 (9th Cir. 1988) (holding that a court “may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction”). Once a party has moved to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the opposing party bears the burden of establishing the Court’s jurisdiction. See Kokkonen v. Guardian Life Ins. Co., 511 U.S. 375, 377 (1994); Chandler v. State Farm Mut. Auto. Ins. Co., 598 F.3d 1115, 1122 (9th Cir. 2010).
b. Motion to dismiss under Rule 12(b)(6) and Rule 9(b)

A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A motion to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure tests the legal sufficiency of the claims asserted in the complaint. Fed. R. Civ. P. 12(b)(6); Navarro v. Block, 250 F.3d 729, 731 (9th Cir. 2001). The court must accept all factual allegations pleaded in the complaint as true, and must construe them and draw all reasonable inferences from them in favor of the nonmoving party. Cahill v. Liberty Mutual Ins. Co., 80 F.3d 336, 337–38 (9th Cir. 1996). The Court is not bound, however, to accept “legal conclusions” as true. Ashcroft v. Iqbal, 556 U.S. 662 (2009).

To avoid a Rule 12(b)(6) dismissal, a complaint need not contain detailed factual allegations; rather, it must plead “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). However, “a plaintiff’s obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” Id. at 555 (citation omitted). “Factual allegations must be enough to raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true (even if doubtful in fact).” Id. (citation omitted). In spite of the deference the court is bound to pay to the plaintiff’s allegations, it is not proper for the court to assume that “the [plaintiff] can prove facts that [he or she] has not alleged or that defendants have violated the . . . laws in ways that have not been alleged.” Associated Gen. Contractors of Cal., Inc. v. Cal. State Council of Carpenters, 459 U.S. 519, 526 (1983).

But “[w]hen there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief.” Iqbal, 556 U.S. at 679. A claim has “facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. at 677 (citing Twombly, 550 U.S. at 556). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.”
Id. “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’” Id. (quoting Twombly, 550 U.S. at 557).

Complaints alleging fraud must satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). Rule 9(b) requires that in all averments of fraud or mistake, the circumstances constituting fraud or mistake shall be stated with particularity. Malice, intent, knowledge, and other conditions of a person’s mind may be alleged generally. A pleading is sufficient under Rule 9(b) if it “state[s] the time, place and specific content of the false representations as well as the identities of the parties to the misrepresentation.” Misc. Serv. Workers, Drivers & Helpers v. Philco–Ford Corp., 661 F.2d 776, 782 (9th Cir. 1981) (citations omitted); see also Vess v. Ciba–Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting Cooper v. Pickett, 137 F.3d 616, 627 (9th Cir. 1997)) (“Averments of fraud must be accompanied by ‘the who, what, when, where, and how’ of the misconduct charged.”) Additionally, “the plaintiff must plead facts explaining why the statement was false when it was made.” Smith v. Allstate Ins. Co., 160 F.Supp.2d 1150, 1152 (S.D. Cal. 2001) (citation omitted); see In re GlenFed, Inc. Sec. Litig., 42 F.3d 1541, 1549 (9th Cir. 1994) (en banc) (superseded by statute on other grounds).

Regardless of the title given to a particular claim, allegations grounded in fraud are subject to Rule 9(b)’s pleading requirements. See Vess, 317 F.3d at 1103–04. Even where fraud is not an essential element of a consumer protection claim, Rule 9(b) applies where a complaint “rel[ies] entirely on [a fraudulent course of conduct] as the bases of that claim . . . the claim is said to be ‘grounded in fraud’ or to ‘sound in fraud,’ and the pleading . . . as a whole must satisfy the particularity requirement of Rule 9(b).” Kearns v. Ford Motor Co., 567 F.3d 1120, 1125 (9th Cir. 2009) (quoting Vess, 317 F.3d at 1103–04); Bros. v. Hewlett–Packard Co., 2006 WL 3093685, at *7 (N.D. Cal. Oct. 31, 2006).
III. DISCUSSION

LinkedIn moves to dismiss all claims in the SAC for lack of standing pursuant to Rule 12(b)(1) and failure to state a claim pursuant to Rule 12(b)(6).

The SAC contains three claims for: 1) violation of the fraud prong of California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code, § 17200 et seq., 2) violation of the unfair prong of the UCL, and 3) breach of contract. Plaintiff concedes that her second and third claims should be dismissed and asks that the Court do so without prejudice. Docket No. 87, Pl.’s Opp. Brief at 3. LinkedIn asks that the Court dismiss all three claims with prejudice.

For the reasons explained below, the Court DISMISSES Plaintiff’s second and third claims with prejudice. LinkedIn’s motion is DENIED as to Plaintiff’s first claim.

a. Standing under Article III and the UCL

i. Background

The Court dismissed Plaintiff’s First Amended Complaint (“FAC”) for lack of Article III standing. See Docket No. 72. Plaintiff had attempted to establish standing based on the theories that she had suffered an injury in fact because 1) she did not receive the benefit of her bargain with LinkedIn, and 2) she now faces an increased risk of future harm as a result of the 2012 hacking incident. The Court rejected both standing theories, finding, inter alia, that the promise of industry standard security had not been a part of Plaintiff’s bargain for premium services.

The parties continue to dispute whether Plaintiff has standing under Article III or under the UCL. Plaintiff has abandoned the standing theories she previously advanced and now contends that she has standing because she purchased her premium subscription in reliance on LinkedIn’s misrepresentation and would not have done so but for the misrepresentation. Importantly, the SAC (unlike the FAC) alleges that Plaintiff did, in fact, read and rely upon the statement in the Privacy Policy regarding industry standard security.

With these amendments, the SAC’s allegations are sufficient to confer both standing under Article III and statutory standing under the UCL.
ii. The parties’ positions

The parties essentially divide the UCL standing and Article III standing cases into two categories. Plaintiff relies primarily on a line of cases in which courts find standing under the UCL and under Article III for plaintiffs who purchase deceptively labeled or advertised products in reliance on the misinformation contained in the labels or advertisements.

As to UCL standing, in Kwikset Corp. v. Superior Court, the California Supreme Court held that “[a] consumer who relies on a product label and challenges a misrepresentation contained therein can satisfy the standing requirement of [the UCL] by alleging . . . that he or she would not have bought the product but for the misrepresentation.” 51 Cal. 4th 310, 330 (2011). In Hinojos v. Kohl’s Corp., 718 F.3d 1098 (9th Cir. 2013), the Ninth Circuit Court of Appeals applied Kwikset in “a straightforward manner” to hold that “when a consumer purchases merchandise on the basis of false price information, and when the consumer alleges that he would not have made the purchase but for the misrepresentation, he has standing to sue under the UCL and FAL because he has suffered an economic injury.” 718 F.3d at 1107.

The Article III standing cases in the Ninth Circuit agree that plaintiffs who make allegations similar to those made in Kwikset and Hinojos would also satisfy Article III’s standing requirements. For example, Article III standing has been found for class members who “paid more for [a product] than they otherwise would have paid, or bought it when they otherwise would not have done so, because [the defendant] made deceptive claims and failed to disclose the [product’s] limitations.” Mazza v. Am. Honda Motor Co., Inc., 666 F.3d 581, 595 (9th Cir. 2012) (citing Stearns v. Ticketmaster Corp., 655 F.3d 1013, 1021 (9th Cir. 2011)). Another Ninth Circuit case found Article III standing by applying the rule from Kwikset to the plaintiffs’ allegation that they paid more for a product due to reliance on false advertising. See Degelmann v. Advanced Med. Optics, Inc., 659 F.3d 835, 840 (9th Cir. 2011) vacated, 699 F.3d 1103 (9th Cir. 2012).

LinkedIn, on the other hand, distinguishes the labeling/advertising cases on the basis that the representation in the Privacy Policy was not contained in a label or an advertisement. The Privacy Policy applies to all members, both paying and non-paying and, according to LinkedIn,
was not included or incorporated into the premium services contract that Plaintiff entered into.

Thus, LinkedIn argues, “[u]nder no plausible theory can this single sentence in the Privacy Policy that applies to all LinkedIn members be considered an ‘inducement’ to the purchase of a premium subscription, the ‘advertisement’ of premium services, or an ‘effective marketing technique’ for premium service.” Docket No. 89, Def.’s Reply at 7.

LinkedIn instead points to a number of other consumer cases in which courts have rejected theories of injury in fact that, like Plaintiff’s theory, were premised on payment or overpayment for a product. In LinkedIn’s cases, courts have required plaintiffs to allege “something more” than “overpaying for a ‘defective’ product” in order to establish an Article III injury in fact. In re Toyota Motor Corp., 790 F. Supp. 2d 1152, 1165 n.11 (C.D. Cal 2011); see also Whitson v. Bumbo, 2009 WL 1515597 (N.D. Cal. Apr. 16, 2009); Boysen v. Walgreen Co., 2012 WL 2953069 (N.D. Cal. July 19, 2012); In re McNeil Consumer Healthcare, 877 F. Supp. 2d 2d 254 (E.D. Pa. 2012); Williams v. Purdue Pharma Co., 297 F. Supp. 2d 171 (D.D.C. 2003). Based on these cases, LinkedIn contends that Plaintiff has not alleged sufficient facts to establish Article III standing.

LinkedIn argues that the rationale behind the labeling/advertising cases is that “the overpayment injury does not depend on how the product functions because ‘labels’ and ‘brands’ have independent economic value.” In re Toyota, 790 F. Supp. 2d at 1165 n.11. Based on that rationale, LinkedIn argues, courts in such cases find economic harm when the consumer paid money for a defendant’s product over a competitor’s product due to the mislabeling. Plaintiff makes no such allegations here. She does not allege, for example, that she purchased LinkedIn’s services over another networking website’s services because of the promise regarding industry standard security.

**iii. Application and conclusion**

Having carefully considered the cases, the Court finds that Plaintiff has alleged facts sufficient to confer standing. The critical distinction between Plaintiff’s theory of economic injury and the theories of economic injury rejected in LinkedIn’s cited cases is that Plaintiff alleges her...
payment or overpayment was caused by LinkedIn’s alleged misrepresentations, which she alleges she read and relied on in making her decision to purchase a premium subscription. The plaintiffs in LinkedIn’s cases did not, or could not, attempt to establish standing under the same theory as Plaintiff’s. In Williams and Whitson, although the plaintiffs alleged that the defendants had made misrepresentations about the products at issue, the plaintiffs failed to allege that they were deceived by or even that they were exposed to the misrepresentations. 297 F. Supp. 2d at 177; 2009 WL 1515597, at *4. Similarly, neither Boysen nor In re McNeil contained allegations that the plaintiffs purchased the product in reliance on the defendant’s misrepresentations. In re Toyota is inapposite because, while the court did require some plaintiffs to allege “something more” than pure economic loss, it did so only for those plaintiffs who were seeking to establish an economic loss based on a “market effect” theory. 3 790 F. Supp. 2d at 1165-1166. Plaintiff’s theory is not based on a loss in market value.

The Court recognizes that there are significant differences between the “single sentence” contained in LinkedIn’s Privacy Policy and the labels and advertisements from Kwikset and Hinojos. Notwithstanding these differences, however, the Court finds that the representation in LinkedIn’s Privacy Policy falls within the scope of the labeling/advertising cases.

First, it is not clear that the reach of the Kwikset line of cases is limited only to misrepresentations that are also labels or advertisements. As the California Supreme Court put it, to satisfy the UCL’s standing requirements, “a party must now (1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., economic injury, and (2) show that that economic injury was the result of, i.e., caused by, the unfair business practice or false advertising that is the gravamen of the claim.” Kwikset, 51 Cal. 4th at 322 (emphasis added). While it is true that the final holding in Kwikset specifically identified the type of “unfair business

3 Some plaintiffs attempted to establish an injury in fact based on a drop in value of their cars. They did not allege experiencing any defects in their cars despite predicing their loss on the drop in value due to the defect. The court agreed that those plaintiffs should allege “something more” and found that they had met this requirement by 1) showing the reduction in trade-in value of their cars in sources such as Kelley Blue Book and 2) alleging that the drop in value followed public awareness of the defect. 790 F. Supp. 2d at 1166.
practice or false advertising” at issue\(^4\), that holding was an application of the broader rule identified in the preceding sentence of this paragraph. The *Kwikset* court did not indicate that the requirements for establishing UCL standing would be any different if the challenged misrepresentation was contained in something other than a deceptive product label. And although *Kwikset* was a California case concerning standing under the UCL, not Article III, the Ninth Circuit cases indicate that plaintiffs whose allegations meet the *Kwikset* criteria will at least satisfy the Article III injury in fact requirement. See *Hinojos*, 718 F.3d at 1104, n.3 (“There is no difficulty in this case regarding Article III injury in fact, and neither party suggests otherwise. We have explained that when, as here, ‘Plaintiffs contend that class members paid more for [a product] than they otherwise would have paid, or bought it when they otherwise would not have done so’ they have suffered an Article III injury in fact.”)

Second, even if the *Kwikset* line of cases was read to apply solely to advertisements and labels, the term “advertisement” is defined broadly under California law. The UCL expressly incorporates the Fair Advertising Law’s (“FAL”) prohibition on unfair advertising as one form of unfair competition. *Hinojos*, 718 F.3d at 1103 (citing Cal. Bus. & Prof. Code § 17200). The FAL is broadly written and broadly construed, and a wide range of statements can qualify as an advertisement. Cal. Bus. & Prof. Code § 17500; see *Chern v. Bank of Am.*, 15 Cal. 3d 866, 875 (1976). For example, a statement made in a letter denying a borrower’s request for a loan modification qualifies as “advertising.” *Gabali v. OneWest Bank, FSB*, 2013 WL 1320770 (N.D. Cal. Mar. 29, 2013). Applying one set of standing requirements to labeling/advertising and another set of standing requirements to other types of misrepresentations, as LinkedIn advocates, would be untenable given the lack of distinction California law places between misleading advertising and other forms of misleading statements.

The opinions in *Kwikset* and *Hinojos* provided several examples of marketing practices, including meat labeled as kosher and a product advertised as “not available in stores.” Like those

\(^4\)“A consumer who relies on a product label and challenges a misrepresentation contained therein can satisfy the standing requirement of section 17204 by alleging, as plaintiffs have here, that he or she would not have bought the product but for the misrepresentation.” *Id.* at 330.
examples, the statement in LinkedIn’s Privacy Policy might be significant only to a small segment of consumers and many consumers may not even care to read it before making their purchase. Yet the California Supreme Court and the Ninth Circuit Court of Appeals have indicated that when those representations are false, a consumer who is induced by them to purchase a product that she otherwise would not have purchased has standing to bring an action under the UCL in federal court.

Applying the cases discussed above, the Court finds that Plaintiff’s allegations are sufficient to establish standing under the UCL and Article III. She alleges that she purchased her premium subscription on the basis of LinkedIn’s statement that its users’ data will be secured with industry standards and technology, she alleges that the statement was false when she read and relied on it, and she alleges that she would not have made the purchase (or that she would have negotiated for a lower price) but for the misrepresentation. Her injury (the purchase induced by the misrepresentation) is fairly traceable to LinkedIn’s conduct because LinkedIn made the misrepresentation. And finally, her injury is likely to be redressed by a favorable decision because restitution is an available remedy under the UCL. Cal. Bus. & Prof. Code § 17203.

b. Plaintiff’s first claim: Fraudulent business practices

i. Stating a claim

To state a claim under either the fraudulent business practices prong of the UCL, it is necessary only to show that members of the public are likely to be deceived. In re Tobacco II Cases, 46 Cal. 4th 298, 312 (2009) (internal quotations and citations omitted).

Plaintiff alleges that the representation in the Privacy Policy is likely to deceive the public because consumers would believe that LinkedIn used a more effective method of securing its users’ data than it actually did.

LinkedIn attacks the materiality of the alleged misrepresentation, arguing that Plaintiff’s claim should fail as a matter of law because “it is implausible that a single contractual promise in a Privacy Policy applicable to all members—free, basic-account members and paying, premium-
account members—would be seen as a material inducement leading a reasonable user to upgrade to a premium account.”

A representation is material if a reasonable consumer would attach importance to it or if the maker of the representation knows or has reason to know that its recipient regards or is likely to regard the matter as important in determining his choice of action. *Hinojos*, 718 F.3d at 1107 (internal quotations and citations omitted). The materiality of a misrepresentation is typically an issue of fact, and therefore should not be decided at the motion to dismiss stage. See *In re Steroid Hormone Product Cases*, 181 Cal. App. 4th 145 (2010). In some circumstances, courts have found, as a matter of law, that no reasonable consumer could have been misled by the misrepresentation. See *Rice v. Fox Broad. Co.*, 330 F.3d 1170, 1181 (9th Cir. 2003) (false statements on videotape cover were immaterial because videotape cover could not be observed by potential consumer and therefore could not influence the purchasing decision).

LinkedIn points out that Plaintiff fails to allege that, even if LinkedIn had disclosed the fact that it used unsalted, SHA-1 encryption, Plaintiff would have actually understood such a disclosure to mean that LinkedIn was not employing industry standard security. However, Plaintiff does allege that if LinkedIn had disclosed its security protocols, consumers would have learned that those protocols did not meet the “industry standard” through word of mouth or the media. She supports this reasoning by arguing, essentially, that even if the average consumer would not have understood that unsalted, SHA-1 encryption was below the industry standard, the popular media would have found that disclosure newsworthy and would have disseminated the information to consumers.

Given the above, the Court does not find Plaintiff’s claim barred as a matter of law. The only case that LinkedIn has cited on this point is *Rice*, and in *Rice*, it was impossible for the representation to deceive a consumer when no consumer could have viewed the representation prior to making a purchase. Here, the representation was available for the public to read, and, as explained below, Plaintiff has alleged a plausible explanation for why it is likely to deceive the public.
ii. Rule 8

LinkedIn contends that the SAC does not satisfy Rule 8 of the Federal Rules of Civil Procedure. A complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A court considering a motion to dismiss can choose to begin by identifying pleadings that, because they are no more than conclusions, are not entitled to the assumption of truth. Iqbal, 556 U.S. at 679. While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations. Id. When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief. Id.

1. Whether Plaintiff plausibly alleges that she read LinkedIn’s representation

In the SAC, Plaintiff alleges the following: “Before signing up for her LinkedIn Premium Subscription, Wright—as she always does when signing up for a service online—read and agreed to the [User Agreement] and Privacy Policy and the representations and obligations listed therein.” Plaintiff also alleges that the User Agreement contained an integration clause, and that the User Agreement governing her premium subscription also “incorporated by reference” LinkedIn’s Privacy Policy and advised her to review and comply with the Privacy Policy.

LinkedIn argues that because the User Agreement was not part of the terms of the contract Plaintiff entered into when she signed up for her premium subscription, the terms therefore did not include the “incorporation by reference” term or the advisement to review the Privacy Policy. Because those allegations are false, LinkedIn continues, there is no reason to accept as true the conclusion—that Plaintiff read and relied on the Privacy Policy in purchasing her premium subscription.

However, regardless of whether or not the User Agreement became a part of Plaintiff’s contract for the premium subscription as a matter of contract law, Plaintiff alleges that she read and relied on the User Agreement and the Privacy Policy before purchasing her premium subscription.
Her understanding of contract law has no bearing on her allegation that she read and relied on those documents.

2. Whether Plaintiff plausibly alleges that LinkedIn’s representation was false

LinkedIn argues that Plaintiff’s allegation that LinkedIn failed to use industry standards to encrypt member passwords is conclusory and unsupported. Plaintiff supports this conclusion with the following factual allegations:

1) When Plaintiff purchased her premium subscription, LinkedIn protected its users’ personal information using the SHA-1 hash function. LinkedIn did not salt the information.

2) Since at least 2006, industry standards have required that users’ personal information, and login credentials in particular, be stored in salted and hashed format.

3) The National Institute of Standards and Technology (“NIST”) recommended that all government agencies stop using SHA-1.

4) Salting has been standard encryption practice since the 1970s, and salting and hashing (with a stronger algorithm than SHA-1) together is the preferred industry practice.

5) Three days after the breach, LinkedIn stated that it would transition from a password database system that hashed passwords, i.e. provided one layer of encoding, to a system that both hashed and salted the passwords, i.e. provided an extra layer of protection that is a widely recognized best practice within the industry.

6) The bare minimum practice within LinkedIn’s industry is to “salt” the input before hashing it, preferably with a multi-digit salt long enough to render rainbow tables (a method of encryption-breaking) entirely useless.
The more common industry practice is to (1) salt passwords and then hash them using a more recent and secure algorithm than SHA-1, (2) salt the resulting hash value, and (3) then again run the resulting value through a hashing function. Finally, that fully encrypted password should be stored on a separate and secure server apart from all other user information.

LinkedIn points out that “Plaintiff never explicitly alleges that SHA-1 was below industry standards during the class period. She instead alleges that the National Institute of Standards and Technology [NIST] recommended that all government agencies stop using SHA-1.” Docket No. 81, Def.’s Memo ISO MTD at 19 (internal quotations omitted). LinkedIn then cites to an extrinsic document written by the NIST which purportedly states that the use of SHA-1 hashing is acceptable.

However, even assuming that the Court must disregard Plaintiff’s allegations concerning the NIST’s position on the use of SHA-1 hashing, the rest of Plaintiff’s allegations are sufficient to support her conclusion that LinkedIn’s representation was false. She alleges that LinkedIn used a particular security practice, is specific about what that security practice entailed, alleges that LinkedIn’s practice fell below the “bare minimum” security practice in LinkedIn’s industry, and she is specific about what that “bare minimum” security practice entails. Furthermore, LinkedIn does not contend that the phrase “industry standard” amounts to puffery or is otherwise impossible to define.

Accordingly, dismissal for this reason is unwarranted.

3. Whether Plaintiff plausibly alleges that she was denied the benefit of her bargain

Next, LinkedIn contends that Plaintiff “does not plausibly allege that she did not receive all of the benefits that she bargained for,” arguing that the promise of industry standard security was not one of the benefits included in Plaintiff’s bargain because industry standard security is available to all members whether or not they have upgraded to premium memberships. This was
an argument that the Court found convincing and became one of the grounds for dismissal of the
FAC.

This contention is less relevant now that Plaintiff no longer seeks to establish standing
based on being deprived of the benefit of her bargain. Furthermore, when a plaintiff alleges
economic injury based on being induced by misrepresentations to purchase products that she would
not otherwise have purchased, the benefit of the bargain defense is permissible only if the
misrepresentation that the consumer alleges was not “material.” Hinojos, 718 F.3d at 1107. Thus,
LinkedIn’s contention that Plaintiff received all of the benefits she bargained for is not a sufficient
basis for dismissal of the SAC.

iii. Rule 9

LinkedIn contends that the SAC’s averments of fraud do not satisfy Rule 9(b) after
disregarding the allegations discussed above on Rule 8 grounds. However, these allegations are
sufficiently pleaded and must be regarded as true at this stage in the proceedings.

In alleging fraud or mistake, a party must state with particularity the circumstances

LinkedIn’s averments of fraud meet the requirements of Rule 9(b). She alleges that the
representation was made in LinkedIn’s Privacy Policy, which she read and relied on prior to
purchasing a premium subscription, and she alleges facts that explain why the representation was
false. Her allegations are specific enough to give LinkedIn “notice of the particular misconduct
which is alleged to constitute the fraud charged so that [it] can defend against the charge and not
just deny that [it has] done anything wrong.” Semegen v. Weidner, 780 F.2d 727, 731 (9th Cir.
1985).

c. Plaintiff’s second and third claims

As to the SAC’s second and third claims, the Court limits its decision to whether these
claims should be dismissed with or without prejudice.

Dismissal with prejudice and without leave to amend is not appropriate unless it is clear on
that the complaint could not be saved by amendment. Chang v. Chen, 80 F.3d 1293, 1296 (9th Cir.
1996). Dismissal with prejudice may be appropriate where a plaintiff presents no new facts but
only “new theories” and “provided no satisfactory explanation for his failure to fully develop his
contentions originally.” Vincent v. Trend Western Technical Corp., 828 F.2d 563, 570-71 (9th Cir.
1987).

Here, although Plaintiff has added new, critical facts to her complaint (particularly, the
allegation that she read LinkedIn’s representation before purchasing her premium subscription),
she fails to explain how the new facts affect her second and third claims. She concedes that both
claims fall within the scope of the Court’s previous order dismissing the FAC. She provides no
explanation for why she should be given another chance to amend those claims, other than that she
only became aware that her second and third claims fell within the scope of the previous dismissal
order after certain evidence was produced by LinkedIn and that she might discover facts through
discovery that would allow her to reassert the claims.

Accordingly, Plaintiff’s second and third claims are DISMISSED with prejudice because
allowing for further amendment would be futile.

IV. CONCLUSION

For the foregoing reasons, LinkedIn’s Motion to Dismiss Plaintiff’s Second Amended
Consolidated Complaint is GRANTED IN PART and DENIED IN PART. Plaintiff’s second and
third claims are DISMISSED with prejudice. LinkedIn’s Motion is DENIED as to Plaintiff’s first
claim.

The court schedules this action for a Case Management Conference at 10:00 a.m. on June 6,

IT IS SO ORDERED

Dated: March 28, 2014

[Signature]

EDWARD J. DAVILA
United States District Judge
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

ORDER GRANTING IN PART AND DENYING IN PART
DEFENDANTS’ MOTIONS TO DISMISS

Re: ECF Nos. 393, 394, 395, 396

THIS DOCUMENT RELATES TO ALL CASES
I. Background ........................................................................................................... 1
   A. The App Store ................................................................................................. 3
   B. The Subject Apps ......................................................................................... 5
   C. Apple’s Representations ............................................................................... 7
II. Legal Standards .................................................................................................. 8
III. Apple’s Motion to Dismiss .............................................................................. 10
   A. Article III Standing ..................................................................................... 10
   B. Communications Decency Act ................................................................. 18
   C. Misrepresentation Claims ........................................................................... 23
   D. California Comprehensive Computer Data Access and Fraud Act .............. 34
   E. Strict Products Liability: Design Defect and Failure to Warn ...................... 36
   F. Negligence .................................................................................................. 37
   G. RICO .......................................................................................................... 37
   H. Aiding and Abetting .................................................................................... 37
IV. App Defendants’ Motions to Dismiss .............................................................. 38
   A. Article III Standing ..................................................................................... 38
   B. Plaintiffs’ UCL Claims ................................................................................ 41
   C. Invasion of Privacy: Intrusion Upon Seclusion ........................................... 41
   D. Invasion of Privacy: Public Disclosure of Private Facts ............................... 47
   E. CDAFA and Computer Fraud and Abuse Act ........................................... 48
   F. Electronic Communications Privacy Act ..................................................... 48
   G. Texas and California Wiretap Statutes ......................................................... 49
   H. Texas Theft Liability Act ............................................................................ 50
   I. RICO and Vicarious Liability ...................................................................... 50
V. Facebook and Gowalla’s Motion to Dismiss .................................................... 50
   A. Uniform Fraudulent Transfer Act ............................................................... 51
   B. Successor Liability ...................................................................................... 53
   C. Aiding and Abetting ................................................................................... 54
VI. Conclusion ........................................................................................................ 55
Before the Court are four motions to dismiss filed by Defendants in this action. The operative Consolidated Amended Class Action Complaint ("CAC"), ECF No. 362, collects the claims of fifteen plaintiffs\(^1\) in four related actions against a total of fifteen Defendants. Defendant Apple Inc. designs and manufactures the iPhone, the iPod touch, and the iPad, ("iDevices"), each of which is a mobile device that can wirelessly access the Internet. Since 2008, those devices have included an App Store, which enables users to download software, or apps, to their devices created by third parties. Each Defendant except for Apple is an app developer\(^2\) (collectively, "App Defendants"). Plaintiffs allege that the App Defendants’ apps have been surreptitiously stealing and disseminating the contact information stored by customers on Apple devices. CAC ¶ 7.

I. BACKGROUND

Plaintiffs bring this action on their own behalf, on behalf of an “iDevice Class,” composed of all purchasers of Apple’s iDevices between July 10, 2008 and the present who downloaded the App Defendants’ apps, and on behalf of three subclasses: the “Malware Subclass,” the “Address Book Subclass,” and the “Texas Subclass.” CAC ¶ 48. The Malware Subclass comprises those who downloaded the subject apps. The Address Book Subclass comprises those in the Malware Subclass whose iDevice, without requesting prior approval, “transmitted, disclosed, and/or disseminated the iDevice’s mobile address book (or substantial portions thereof) over the Internet and/or to third-parties” due to the subject apps.

The CAC asserts several overlapping claims against different Defendants on behalf of different Plaintiffs. In total, the CAC asserts the following statutory claims: violation of California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof.s Code § 17200, et seq.; violation

---

1 The sixteenth Plaintiff, Haig Arabian, has voluntarily dismissed his claims. ECF No. 426. The remaining Plaintiffs are Alan Beuershasen, Giuli Biondi, Lauren Carter, Steve Dean, Stephanie Dennis-Cooley, Jason Green, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali Mandaywala, Claire Moses, Judy Paul, Maria Pirozzi, Theda Sandiford and Greg Varner.


The following chart shows which claims each Plaintiff asserts against each Defendant:

<table>
<thead>
<tr>
<th>Cause of Action</th>
<th>On Behalf of</th>
<th>Against</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 UCL</td>
<td>All Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>2 UCL</td>
<td>Opperman Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>3 UCL</td>
<td>Plaintiffs Except Pirozzi</td>
<td>App Defendants</td>
</tr>
<tr>
<td>4 FAL</td>
<td>All Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>5 FAL</td>
<td>Opperman Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>6 CLRA</td>
<td>All Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>7 CLRA</td>
<td>Opperman Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>8 Negligent Misrepresentation</td>
<td>All Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>9 Negligent Misrepresentation</td>
<td>Opperman Plaintiffs</td>
<td>Apple</td>
</tr>
</tbody>
</table>

3 Plaintiffs, Apple, and the App Defendants discuss California and Texas common law interchangeably without explanation, often pointing out that both states’ common law is identical with respect to the issues presented by Defendants’ motions to dismiss. The Court has not identified any differences between Texas and California common law on the issues addressed in this Order, and therefore, for the sake of convenience, discusses only California law.
<table>
<thead>
<tr>
<th>Cause of Action</th>
<th>On Behalf of</th>
<th>Against</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 CDAFA</td>
<td>Plaintiffs Except Pirozzi</td>
<td>All Defendants</td>
</tr>
<tr>
<td>11 CFAA</td>
<td>Plaintiffs Except Pirozzi</td>
<td>App Defendants</td>
</tr>
<tr>
<td>12 ECPA</td>
<td>Plaintiffs Except Pirozzi</td>
<td>App Defendants</td>
</tr>
<tr>
<td>13 Wiretap/Invasion of Privacy Act</td>
<td>CAD Plaintiffs</td>
<td>Foodspotting, Instagram, Path, Twitter, and Yelp</td>
</tr>
<tr>
<td>14 Texas Wiretap Acts</td>
<td>Texas Plaintiffs</td>
<td>App Defendants</td>
</tr>
<tr>
<td>15 Intrusion Upon Seclusion</td>
<td>Opperman Plaintiffs</td>
<td>App Defendants</td>
</tr>
<tr>
<td>16 Public Disclosure of Private Facts</td>
<td>Opperman Plaintiffs</td>
<td>App Defendants</td>
</tr>
<tr>
<td>17 Conversion</td>
<td>Plaintiffs Except Pirozzi</td>
<td>All Defendants</td>
</tr>
<tr>
<td>18 Trespass to Property</td>
<td>Opperman Plaintiffs</td>
<td>All Defendants</td>
</tr>
<tr>
<td>19 Texas Theft Liability Act</td>
<td>Texas Plaintiffs</td>
<td>App Defendants</td>
</tr>
<tr>
<td>20 Misappropriation</td>
<td>Opperman Plaintiffs</td>
<td>App Defendants</td>
</tr>
<tr>
<td>21 Strict Products Liability: Design</td>
<td>Opperman Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>Defect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22 Strict Products Liability: Failure</td>
<td>Opperman Plaintiffs</td>
<td>Apple</td>
</tr>
<tr>
<td>to Warn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23 Negligence</td>
<td>Plaintiffs Except Pirozzi</td>
<td>All Defendants</td>
</tr>
<tr>
<td>24 Uniform Fraudulent Transfer Act</td>
<td>Gowalla Plaintiffs</td>
<td>Gowalla and Facebook</td>
</tr>
<tr>
<td>25 RICO</td>
<td>Opperman Plaintiffs</td>
<td>All Defendants</td>
</tr>
<tr>
<td>26 Secondary and Vicarious Liability</td>
<td>Opperman Plaintiffs</td>
<td>All Defendants</td>
</tr>
</tbody>
</table>

The following summary of Plaintiffs’ allegations is taken from the complaint. As it must, the Court accepts the CAC’s allegations as true for purposes of this motion.

A. The App Store

Apple launched the App Store in 2008, and heavily promoted it in conjunction with its iDevices. CAC ¶ 57. The promotion was successful: the App Store today has over 700,000 apps for iPhone and iPod touch, and 275,000 apps for the iPad. Since 2008, customers have downloaded over forty billion apps. Id.

Apple maintains “exclusive domain” and “ultimate control” over the App Store’s

4 “CAD” Plaintiffs are those who downloaded apps from Foodspotting, Instagram, Path, Twitter, and Yelp.

5 The Texas Plaintiffs are Beuershasen, Biondi, Dean, Hodgins, Hoffman, King, and Varner.
offerings. iDevices are designed only to accept apps from the App Store, and Apple decides which apps will be offered, and which will not. CAC ¶ 60. iDevices also come with pre-programmed apps built into the device’s operating system. Among those apps is Apple’s “Contacts” app — a virtual address book. The App Store is another one. CAC ¶ 61. Neither of these built-in apps can be removed by the user.

“Apple claims to review each application before offering it to its users, purports to have implemented apps privacy standards, and claims to have created a strong privacy protection for its customers.” CAC ¶ 62. However, some apps offered on the App Store are alleged to have accessed and uploaded information from customers’ iDevices without their knowledge, including contact information. Plaintiffs allege that Apple has failed to safeguard the App Store from such apps, while representing to the public that Apple’s products are “safe and secure.” CAC ¶ 64.

Apple is “notorious for complete control over its products.” CAC ¶ 87. App developers must submit their apps to Apple for review, and Apple decides whether to offer them on the App Store. To be eligible for inclusion, third-party app developers must register with Apple and agree to the iOS Developer Agreement ("IDA") and the Program License Agreement ("PLA"), as well as pay a yearly registration fee. CAC ¶¶ 87–89. Apple reserves the right to reject apps for any reason, and has explicitly reserved the right to reject apps that breach the licensing agreements, provide Apple with inaccurate documents or information, or violate, misappropriate, or infringe the rights of a third party. CAC ¶ 90. After joining the program, app developers use Apple’s software development kit ("SDK"), which provides guidelines and tools for app development. CAC ¶ 91.

The App Store Review Guidelines prohibit the transmission of user data without prior permission. CAC ¶¶ 101, 104. However, Plaintiffs allege that Apple’s “iOS Human Interface Guidelines” encourage data theft. The guidelines are meant to guide developers as they create apps for the App Store. Apple tells developers, “don’t force people to give you information you can easily find for yourself, such as their contacts or calendar information,” and “[i]f possible, avoid requiring users to indicate their agreement to your [end user license agreement] when they first start your application. Without an agreement displayed, users can enjoy your application
without delay.” CAC ¶ 212 (emphasis omitted).

Plaintiffs allege that “Apple taught Program registrants’ to incorporate forbidden data harvesting functionalities — even for private “contacts” — into their Apps and encouraged Program registrants to design those functions to operate in non-discriminable manners that would not be noticed by the iDevice owner. These App Defendants, apparently in accord with Apple’s instructions, did just that with their identified Apps.” CAC ¶ 214.

Similarly, Plaintiffs allege: “Apple’s Program tutorials and developer sites [] teach Program registrants how to code and build apps that non-consensually access, manipulate, alter, use and upload the mobile address books maintained on Apple iDevices.” CAC ¶ 190.

B. The Subject Apps

Plaintiffs allege that each of the App Defendants developed an app that copied iDevice users’ contact information without the user’s consent. In February 2012, it was revealed that App Defendant Path’s app, also called “Path,” was uploading users’ contacts and calendar information to its servers without users’ knowledge. Path’s CEO publicly apologized after the practice was made public. CAC ¶ 110.

Plaintiffs allege that several popular apps, including those designed by each App Defendant, have accessed and uploaded user data without consent. In some of these cases, the apps accessed user data without any prompt at all. See CAC ¶¶ 112, 136. Path is one such app. In other cases, the apps “surreptitiously accessed and uploaded information from users’ Contacts app through a ‘Find Friends’ feature without disclosing to users that the feature would leave their private information vulnerable to unauthorized download by the third-party app manufacturer.” CAC ¶ 108.

The public revelations concerning third parties’ access to users’ private information led Congressmen Waxman and Butterfield to write to Apple and to thirty-four app publishers in February and March of 2012, asking for more information about the practice. CAC ¶¶ 115–17

The February letter to Apple noted that Apple’s website at that time represented that iDevice apps “have access to a device’s global data such as contacts in the Address Book,” while Apple’s review guidelines required app developers to gain users’ permission prior to transmitting...
data about a user. CAC ¶ 115. The letter continues:

In spite of this guidance, claims have been made that “there’s a quiet understanding among many iOS app developers that it is acceptable to send a user’s entire address book, without their permission, to remote servers and then store it for future reference. It’s common practice, and many companies likely have your address book stored in their database.” One blogger claims to have conducted a survey of developers of popular iOS apps and found that 13 of 15 had a “contacts database with millions of records” — with one claiming to have a database containing “Mark Zuckerberg’s cell phone number, Larry Ellison’s home phone number and Bill Gates’ cell phone number.

Id. In March 2012, Senator Schumer called for an investigation by the Federal Trade Commission. CAC ¶ 118. In September 2012, Apple released iOS 6, which updated privacy settings on iDevices in a manner that discloses which apps access users’ contacts, calendars, reminders, photos, and other personal information, and allows users a way to prevent certain apps from accessing certain information. CAC ¶ 120.

The following chart outlines the apps each Plaintiff alleges he or she downloaded and deployed:

<table>
<thead>
<tr>
<th>Plaintiff</th>
<th>Angry Birds Classic</th>
<th>Angry Birds</th>
<th>Cut The Rope</th>
<th>Foodspotting</th>
<th>Foursquare</th>
<th>Gowalla</th>
<th>Hipster</th>
<th>Instagram</th>
<th>Kik Messenger</th>
<th>Path</th>
<th>Twitter</th>
<th>Yelp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alan Beuershasen</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Giulì Biondi</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Lauren Carter</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Steve Dean</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stephanie Dennis-Cooley</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jason Green</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Claire Hodgins</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Gentry Hoffman</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Rachelle King</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Nirali Mandaywala</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Claire Moses</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Judy Paul</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Maria Pirozzi</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Theda Sandiford</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Greg Varner</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
C. Apple’s Representations

Plaintiffs allege that “Apple has repeatedly represented that Apple’s products are safe and secure, and that private information could not be accessed by third-party apps without the user’s express consent.” CAC ¶ 64. Throughout the CAC, Plaintiffs identify representations Apple has made on its website, in in-store advertisements, and otherwise, to the effect that iOS is “highly secure,” sometimes in particular with respect to the accessing of data by apps from other apps. See CAC ¶¶ 102–04, 121–123.

For example, when the App Store first launched, Apple’s former CEO Steve Jobs explained, “[t]here are going to be some apps that we’re not going to distribute. Porn, malicious apps, apps that invade your privacy.” CAC ¶ 92. Plaintiffs allege that Apple repeated this refrain continuously during the launch of the App Store, and publicly took action consistent with these goals. See CAC ¶¶ 93–98. In October 2007, Jobs stated: “It will take until February to release an SDK because we’re trying to do two diametrically opposed things at once — provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. As our phones become more powerful, these malicious programs will become more dangerous.” CAC ¶ 94. At an SDK press conference on March 6, 2008, Jobs repeated that Apple would place limitations on third party apps for “malicious” and “illegal” content in order to address “privacy” concerns. CAC ¶ 93. Apple also “famously refused to integrate Adobe Flash technology” despite user demands. Jobs explained in April 2010 that this decision was made “because of reliability, security, and performance concerns.” CAC ¶ 97. “In sum, Apple has attempted to cultivate a perception that its products are safe and that Apple strives to protect users.” CAC ¶ 99.

In September 2011, Apple’s website stated that “iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can’t access data from other apps.” CAC ¶ 102. Apple also assured consumers that, for data-security purposes, “Applications on the device are ‘sandboxed’ so they cannot access data stored by other applications.” CAC ¶ 209.

Apple’s “customer privacy policy” states that Apple takes “precautions — including
administrative, technical, and physical measures — to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.” CAC ¶ 122.

Plaintiffs further allege that “[f]rom 2008 to the present, the highest levels of Apple (from its founder to its current CEO to its corporate spokespersons) have so consistently expressed publicly that Apple protects its customers’ and iDevice owners’ security and privacy that — though inaccurate — it is ingrained into the image of Apple’s culture, products and offerings as well as in the minds of customers.” CAC ¶ 211.

Plaintiffs allege they saw and relied on Apple’s website, in-store advertisements, and television advertising in purchasing their iDevices, and that they would have paid less for their devices, or not purchased them at all, had they known they were vulnerable to privacy attacks. See CAC ¶ 125–26.

II. LEGAL STANDARDS

On a motion to dismiss, the Court accepts the material facts alleged in the complaint, together with all reasonable inferences to be drawn from those facts, as true. Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). However, “the tenet that a court must accept a complaint’s allegations as true is inapplicable to threadbare recitals of a cause of action’s elements, supported by mere conclusory statements.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). To be entitled to the presumption of truth, a complaint’s allegations “must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively.” Starr v. Baca, 652 F.3d 1202, 1216 (9th Cir. 2011), cert. den’d, --- U.S. ----, 132 S.Ct. 2101 (2012).

To survive a motion to dismiss, a plaintiff must plead “enough facts to state a claim to relief that is plausible on its face.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007). Plausibility does not mean probability, but it requires “more than a sheer possibility that a defendant has acted unlawfully.” Iqbal, 556 U.S. at 687. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. In the Ninth Circuit, “[i]f there are two
alternative explanations, one advanced by defendant and the other advanced by plaintiff, both of
which are plausible, plaintiff’s complaint survives a motion to dismiss under Rule 12(b)(6).

Plaintiff’s complaint may be dismissed only when defendant’s plausible alternative explanation is
so convincing that plaintiff’s explanation is implausible.” Starr, 652 F.3d at 1216 (original
emphasis).

In addition, fraud claims are subject to a heightened pleading standard. “In alleging fraud
or mistake, a party must state with particularity the circumstances constituting fraud or mistake.”
Fed. R. Civ. P. 9(b). The allegations must be specific enough to give a defendant notice of the
particular misconduct alleged to constitute the fraud such that the defendant may defend against
the charge. Semegen v. Weidner, 780 F.2d 727, 731 (9th Cir. 1985). In general, allegations
sounding in fraud must contain “an account of the time, place, and specific content of the false
representations as well as the identities of the parties to the misrepresentations.” Swartz v. KPMG
LLP, 476 F.3d 756, 765 (9th Cir. 2007). However, “[m]alice, intent, knowledge, and other
conditions of a person's mind may be alleged generally.” Fed. R. Civ. P. 9(b).

Finally, a “Rule 12(b)(1) jurisdictional attack may be facial or factual. In a facial attack,
the challenger asserts that the allegations contained in a complaint are insufficient on their face to
invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the
allegations that, by themselves, would otherwise invoke federal jurisdiction.” Safe Air for
Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004) (citation omitted). In resolving a facial
attack, courts assume that the allegations are true, and draw all reasonable inferences in the
plaintiff’s favor. Wolfe v. Strankman, 392 F.3d 358, 362 (9th Cir. 2004) (citations omitted). “In
resolving a factual attack on jurisdiction, the district court may review evidence beyond the
complaint without converting the motion to dismiss into a motion for summary judgment. The
court need not presume the truthfulness of the plaintiff’s allegations. Once the moving party has
converted the motion to dismiss into a factual motion by presenting affidavits or other evidence
properly brought before the court, the party opposing the motion must furnish affidavits or other
evidence necessary to satisfy its burden of establishing subject matter jurisdiction.” Safe Air, 373
F.3d at 1039 (citations omitted).
III. APPLE’S MOTION TO DISMISS

Apple moves to dismiss all of Plaintiffs’ claims on Article III standing grounds, as well as each of Plaintiffs’ substantive claims for failure to state a claim upon which relief can be granted. Because Article III standing is a threshold jurisdictional question, the Court will first address Apple’s Rule 12(b)(1) motion to dismiss on the grounds that Plaintiffs lack Article III standing. See Steel Co. v. Citizens for a Better Env., 523 U.S. 83, 94 (1998).

A. Article III Standing

1. Legal Standards

To establish Article III standing, a plaintiff in federal court must meet three requirements. First, the plaintiff must have suffered an “injury in fact” — an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of — the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

The standing requirements are not pleading requirements. Rather, “each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation.” Id. at 561. Nevertheless, “[a]t the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice.” Id. A “court’s obligation to take a plaintiff at its word at that stage in connection with Article III standing issues is primarily directed at the injury in fact and causation issues, not redressability.” Levine v. Vilsack, 587 F.3d 986, 996–97 (9th Cir. 2009) (citing Lujan, 504 U.S. at 561). “[I]t is within the trial court's power to allow or to require the plaintiff to supply, by amendment to the complaint or by affidavits, further particularized allegations of fact deemed supportive of plaintiff's standing.” Warth v. Seldin, 422 U.S. 490, 501–02 (1975).

In addition, even when a plaintiff is able to establish Article III standing, prudential

Finally, in a class action, it is not sufficient for any named plaintiff to rely on the injuries suffered by the class to satisfy Article III standing requirements; each named plaintiff must meet the standing requirements, including satisfactorily alleging that each named plaintiff suffered “non-speculative injury.” Lierboe v. State Farm Mut. Auto. Ins. Co., 350 F.3d 1018, 1022 (9th Cir. 2003).

2. Injury-in-Fact and Causation

Despite the presence of fifteen named Plaintiffs and fifteen Defendants, and the assertion of twenty-six causes of action, Plaintiffs’ case is rather simple. Plaintiffs allege that Apple sold them devices that made it possible for third parties to access and copy Plaintiffs’ address books without their knowledge. Plaintiffs allege, with respect to Apple, that they suffered injury in the form of having overpaid for their iDevices, because they would have paid less for their devices, or not purchased them at all, if Apple had disclosed that it had failed adequately to secure the devices from the alleged intrusion.

In denying Apple’s second motion to dismiss Plaintiff Pirozzi’s claims on standing grounds, this Court observed that her alleged overpayment injury satisfied Article III’s injury-in-fact requirement because “palpable economic injuries have long been recognized as sufficient to lay the basis for standing.” Sierra Club v. Morton, 405 U.S. 727, 733–34 (1972); see also Comm.

Nevertheless, Apple argues that Plaintiffs have not satisfied the causation requirement because no Plaintiff has identified the specific representations made by Apple that form the basis of their overpayment theory of liability. The CAC makes the following allegations concerning Apple’s alleged misrepresentations and Plaintiffs’ reliance:

[E]ach Plaintiff viewed Apple’s online, in-store, and/or television advertisements. In addition, each Plaintiff relied on Apple’s reputation for safety, cultivated through Apple’s extensive marketing and advertising campaigns. Each Plaintiff purchased an iDevice with the expectation that (i) it would come with a fully functioning App Store, and (ii) that Plaintiff would be able to utilize the “Contacts” function and iDevice apps from the App Store without compromising the security, safety, or control of Plaintiff’s iDevice, mobile address book, or other personal and private information. Indeed, each Plaintiff purchased an iDevice with the expectation that he or she would maintain a mobile address book and receive and use additional add-on apps on his or her iDevice. Had any Plaintiff known that iDevices lacked promised features or that Apple designed the iDevices with known vulnerabilities to unauthorized operations from Apple-issued [third-party] apps, Plaintiffs would not have accepted add-on apps from Apple or the App Store and would have paid less for his or her iDevice. At no time prior to the purchase of Plaintiffs’ iDevice did Apple warn any Plaintiff that the iDevice and its data — particularly the Contacts feature and mobile address book — were vulnerable to unauthorized control and dissemination by third-parties.

CAC ¶ 32.

Apple’s standing argument fails to appreciate that “the threshold question of whether plaintiff has standing (and the court has jurisdiction) is distinct from the merits of his claim.
Rather, “[t]he jurisdictional question of standing precedes, and does not require, analysis of the merits.” Maya v. Centex Corp., 658 F.3d 1060, 1068 (9th Cir. 2011) (quoting Equity Lifestyle Props., Inc. v. Cnty. of San Luis Obispo, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008)). In other words, it is possible that Plaintiffs may file a civil action “‘without suffering dismissal for want of standing to sue,’” even though they are “[un]able to assert a cause of action successfully.” In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 n.5 (N.D. Cal. 2011) (quoting Doe v. Chao, 540 U.S. 614, 624–25 (2004)). See also Warth, 422 U.S. at 500 (standing “in no way depends on the merits of the [ ] contention that particular conduct is illegal."); Catholic League for Religious and Civil Rights v. City & Cnty. of San Francisco, 624 F.3d 1043, 1049 (9th Cir. 2010) (en banc) (standing analysis may not “be used to disguise merits analysis, which determines whether a claim is one for which relief can be granted if factually true.”).

For the Court to have jurisdiction over Plaintiffs’ claims, their alleged injury must be “fairly traceable”” to Apple, and not the result of the “‘independent action of some third party not before the court.’” Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992) (quoting Simon v. Eastern Ky. Welfare Rights Organization, 426 U.S. 26, 41–42 (1976)). Plaintiffs’ claims meet that requirement: Plaintiffs allege that Apple misled them through its advertising and failed to disclose material information, that each Plaintiff relied on these misrepresentations or non-disclosures, and that each Plaintiff overpaid for Apple’s products. The requirements to allege standing are not the same as the requirements to plead injury under the substantive law. See Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1027 (N.D. Cal. 2012) (holding plaintiffs satisfied Article III standing even though they had failed to allege reliance on particular representations.

---

7 Apple’s reliance on In re iPhone Application Litig. (“iPhone III”), No. 11-md-2250-LHK, ___ F. Supp. 2d ____, 2013 WL 6212591, at *8 (N.D. Cal. Nov. 25, 2013), underlines the importance of accounting for the stage of litigation at which the Court engages in the standing analysis. After sustaining the plaintiffs’ claims and finding they did not lack standing at the pleading stage, the court in iPhone III granted summary judgment on standing grounds because Apple adduced “specific facts” through discovery that established a lack of evidence of causation, fatally undermining the plaintiffs’ Article III standing. Here, Plaintiffs’ allegations are, at the pleading stage, sufficient to establish standing. That development of the factual record may one day dictate a different result does not alter the Court’s analysis now.
and even though their FAL claims were dismissed with prejudice on that basis).  

Plaintiffs are also independently able to establish standing through their statutory claims because “[t]he injury required by Article III can exist solely by virtue of ‘statutes creating legal rights, the invasion of which creates standing.’” Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010) (quoting Fulfillment Servs., Inc. v. United Parcel Serv., Inc., 528 F.3d 614, 618 (9th Cir. 2008)). See also Robins v. Spokeo, Inc., No. 11-56843, ___ F.3d ___, 2014 WL 407366, at *2–3 (9th Cir. Feb. 4, 2014) (“[T]he violation of a statutory right is usually a sufficient injury in fact to confer standing.”). “The scope of the cause of action determines the scope of the implied statutory right . . . . When, as here, the statutory cause of action does not require proof of actual damages, a plaintiff can suffer a violation of the statutory right without suffering actual damages.” Id. (citation omitted). Apple does not respond to this argument, other than to argue that Plaintiffs cannot establish those substantive claims.

Apple makes several more arguments concerning the merits of Plaintiffs’ claims, including that Plaintiffs have failed to allege their address books were actually uploaded, and that Apple is not responsible for the App Defendants’ conduct. None of these arguments affect the Court’s standing analysis and are better left to the question of whether Plaintiffs have failed to state a claim upon which relief can be granted.

8 There is further support in the CAC for Plaintiffs’ standing. Plaintiffs allege that Apple contributed to the theft of address books through its review of App Store submissions, its App Store review guidelines, its software development kit, other sources of guidance Apple makes available to app developers, and through its failure to catch the offending features contained in the apps implicated in this suit. Plaintiffs also assert product liability claims against Apple for its design of iDevices, and for its failure to warn consumers of their alleged defects. Again, the Court notes that the question of whether these allegations suffice to establish any of Plaintiffs’ claims against Apple is separate from the question of whether these allegations are sufficient to invoke the Court’s subject matter jurisdiction.

9 In fact, the CAC alleges that apps designed by each App Defendant were downloaded by at least one Plaintiff, and that each of those apps has been shown to upload users’ address books without consent after a known set of steps is taken by the user. That Plaintiffs do not allege that their information was, in fact, uploaded is not surprising, since only discovery will reveal whether and how the allegedly widespread practice affected each Plaintiff. But Plaintiffs plausibly allege that they “unwittingly took those steps . . . needed to unwittingly trigger the unnoticeable transmission of their mobile address books.” CAC ¶ 139.
Finally, relying on *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013), Apple argues that an overpayment claim cannot survive without an allegation of “something more” than overpaying for a defective product, such as an allegation that the address books were actually stolen. In *LinkedIn*, the court held that, “in cases where the alleged wrong stems from allegations about insufficient performance or how a product functions, courts have required plaintiffs to allege ‘something more’ than ‘overpaying for a ‘defective’ product.’” *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (citing *In re Toyota Motor Corp.*, 790 F.Supp.2d 1152, 1165 n. 11 (C.D.Cal.2011)).

Apple misreads *LinkedIn* and the cases upon which the *LinkedIn* court relied. The deficiency in the *LinkedIn* plaintiffs’ standing was that they were pleading only a difference between what they had been promised by LinkedIn and what they had received, *i.e.*, a breach of contract. *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (“Plaintiffs cannot rely solely on the ‘benefit of the bargain’ theory of economic harm to sufficiently meet the requirements for Article III standing”). They did not allege that they had suffered any other separate injury.

More relevant here is the decision in *In re Toyota Motor Corp.*, 790 F. Supp. 2d 1152, 1165 (C.D. Cal. 2011), on which the *LinkedIn* court relied. There, the plaintiffs alleged that they relied on Toyota’s “advertisements for Toyota vehicles on television, in magazines, on billboards, in brochures at the dealership, on the Internet, in newspapers, and on banners in front of the dealership,” throughout which “safety and reliability” were a “consistent theme.” *Id.* at 1161. The plaintiffs also alleged that, had Toyota disclosed the safety defect in its vehicles of which they complained, they would not have purchased their vehicles, or would have paid less for them. Relatedly, they alleged that their vehicles were worth less in the used car market as a consequence of the public revelations concerning the safety defect. The *Toyota Motors* court rejected many of the same standing arguments Apple advances here because “once the safety defect is sufficiently and plausibly pled by all Plaintiffs, the economic losses resulting from the defect are readily established: defective cars are simply not worth as much.” *Id.* at 1163. This was so even though the defect had not manifested in all of the plaintiffs’ vehicles. As the *Toyota Motors* court
explained,

When the economic loss is predicated solely on how a product functions, and the product has not malfunctioned, the Court agrees that something more is required than simply alleging an overpayment for a “defective” product . . . . [T]hat “something more” could be allegations based on market forces. It could also be based on sufficiently detailed, non-conclusory allegations of the product defect.

Id. at 1165 n.11.

Here, the Court finds that Plaintiffs’ allegations concerning the offending feature of the product — design that enables third parties to take address book information without consent — supply the “something more” that is required. Whether Plaintiffs’ product liability claims state a claim upon which relief can be granted is a separate question the Court addresses below.

Separately, Plaintiffs allege injury-in-fact to their property rights in their address books, as distinct from the economic injury of overpayment for their iDevices, as support for their common law conversion and trespass claims. The Court discusses this allegation in connection with the App Defendants’ motion to dismiss in more detail infra, Part IV.A. For the reasons discussed in that section, the Court finds that Plaintiffs lack Article III standing based on any injury to their property rights in their address books. For this reason, the Court will dismiss Plaintiffs’ common law claims against Apple for conversion and trespass.

3. Non-Resident Plaintiffs

Apple also argues that the non-resident Plaintiffs lack standing to assert California statutory claims. That argument “conflates two issues: the extraterritorial application of California consumer protection laws (or the ability of a nonresident plaintiff to assert a claim under California law), and choice-of-law analysis . . . .” Forcellati v. Hyland’s, Inc., 876 F. Supp. 2d 1155, 1160 (C.D. Cal. 2012). “Whether a nonresident plaintiff can assert a claim under California law is a constitutional question based on whether California has sufficiently significant contacts with the plaintiff’s claims.” Id. (citing Mazza v. American Honda Motor Co., 666 F.3d 581, 589 (9th Cir. 2012)). In Mazza, for example, “California ha[d] a constitutionally sufficient aggregation of contacts to the claims of each putative class member . . . because Honda’s corporate headquarters, the advertising agency that produced the allegedly fraudulent misrepresentations,
and one fifth of the proposed class members [were] located in California.”  Mazza, 666 F.3d at 589. In Forcellati, the fact that the defendant was alleged to be headquartered in Los Angeles led the court to conclude that “application of California law poses no constitutional concerns.”  Forcellati, 876 F. Supp. 2d at 1160.

Apple’s arguments here were recently rejected by Judge Wilken in another case arising out of Apple’s marketing activities.  See In re iPhone 4S Consumer Litig., No. 12-cv-1127-CW, 2013 WL 3829653, at *7–8 (N.D. Cal. July 23, 2013). There, the plaintiffs “alleged that their injuries were caused by Apple's wrongful conduct in false advertising that originated in California.”  Id. at *7. Judge Wilken noted that the presumption against the extraterritoriality of California law does not apply where the misconduct occurs in California.  See Wershba v. Apple Computer, Inc., 91 Cal. App. 4th 224, 243 (2001) (California statutes apply to “non-California members of a nationwide class where the defendant is a California corporation and some or all of the challenged conduct emanates from California.”). Judge Wilken also distinguished In re Apple & AT&T iPad Unlimited Data Plan Litig., 802 F. Supp. 2d 1070, 1076 (N.D. Cal. 2011), upon which Apple also relies here, because in that case, unlike here, a contractual choice-of-law clause selected the law of each customer’s state of residence. The Court agrees with Judge Wilken’s careful analysis in the iPhone 4S decision.

Apple relies heavily on Sullivan v. Oracle Corp., 51 Cal. 4th 1191, 1209 (2011), for support. Sullivan concerned an overtime claim asserted under the unlawful prong of the UCL, the predicate offense for which was a violation of the federal Fair Labor Standards Act (“FLSA”).

The plaintiffs alleged that the employer had made the decision to mis-classify workers in California. Noting that “the UCL reaches any unlawful business act or practice committed in California,” the court found that “for an employer to adopt an erroneous classification policy is not unlawful in the abstract.”  Id. at 1208. Consequently, the court held that the UCL “does not apply to overtime work performed outside California for a California-based employer by out-of-state plaintiffs in the circumstances of this case based solely on the employer’s failure to comply with

10 The Ninth Circuit had certified the question for the California Supreme Court to answer.
the overtime provisions of the FLSA.” Id. Thus, the California Supreme Court’s holding (1) did not undermine the established presumption that nonresident plaintiffs may assert California claims to address unlawful conduct committed in California by a California resident; and (2) was limited to the FLSA overtime pay context because the work is “performed outside California.” Other courts have come to the conclusion, as this Court does, that Sullivan provides no support for the argument that a national class cannot assert California fraud claims against a California corporation for its misleading marketing. See, e.g., Gross v. Symantec Corp., No. 12-cv-154-CRB, 2012 WL 3116158, at *7 n.10 (N.D. Cal. July 31, 2012); Parkinson v. Hyundai Motor America, 258 F.R.D. 580, 598 (C.D. Cal. 2008).

The Court notes that Apple has not argued that the Court should apply the law of each plaintiff’s home state to her claims, and the Court does not reach the question of whether it should. The Court only concludes that it is constitutional for the nonresident Plaintiffs to assert California statutory claims against Apple based on Apple’s conduct in California. For this reason, Apple’s reliance on the choice-of-law analysis in In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942 (S.D. Cal. 2012), and Frezza v. Google, Inc., No. 12-cv-237-RMW, 2013 WL 1736788, at *5 (N.D. Cal. Apr. 22, 2013), is misplaced. The question of whether the CAC presents a certifiable class under Mazza, and in particular, how a choice-of-law analysis would affect class certification, is a question for another day.

B. Communications Decency Act

Apple moves to dismiss all of Plaintiffs’ claims against it, except those premised on Apple’s alleged misrepresentations, on the ground that the Communications Decency Act (“CDA”), 47 U.S.C. § 230, bars Plaintiffs’ claims. Section 230(c)(1) provides: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Section 230(c)(2) provides:

No provider or user of an interactive computer service shall be held liable on account of--

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or
otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [section 230(c)(1)].

Pursuant to the Act, an “interactive computer service” is “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.” 47 U.S.C. § 230(f)(2). An “information content provider” is “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” 47 U.S.C. § 230(f)(3).

Congress enacted these provisions as part of the Communications Decency Act of 1996 “for two basic policy reasons: to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003). “In light of these concerns, reviewing courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of ‘interactive computer service’ and a relatively restrictive definition of ‘information content provider.’ Under the statutory scheme, an ‘interactive computer service’ qualifies for immunity so long as it does not also function as an ‘information content provider’ for the portion of the statement or publication at issue.” Id. at 1123 (footnotes omitted).

Nevertheless, neither section 230(c) nor any other subsection in the CDA “declares a general immunity from liability deriving from third-party content.” Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100 (9th Cir. 2009). Instead, to determine whether the CDA operates as a bar to civil liability, courts must determine whether “a plaintiff’s theory of liability would treat a defendant as a publisher or speaker of third-party content.” Id. at 1101. “[W]hat matters is not the name of the cause of action — defamation versus negligence versus intentional infliction of emotional distress — what matters is whether the cause of action inherently requires the court to treat the defendant as the ‘publisher or speaker’ of content provided by another. To put it another way, courts must
ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a ‘publisher or speaker.’ If it does, section 230(c)(1) precludes liability.” Id. at 1101–02.

Determining whether a defendant is a “publisher” requires further definition of that term. The Ninth Circuit has held that “publication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content.” Id. at 1102. “[A] publisher reviews material submitted for publication, perhaps edits it for style or technical fluency, and then decides whether to publish it.” Id. Despite Plaintiffs’ arguments to the contrary,11 “it is immaterial whether this decision comes in the form of deciding what to publish in the first place or what to remove among the published material. This is particularly so in the context of the internet, where material can be ‘posted’ and ‘unposted’ with ease.” Id. at 1102 n.8 (citing Batzel v. Smith, 333 F.3d 1018, 1032 (9th Cir. 2003)). Cf. Batzel v. Smith, 333 F.3d 1018, 1032 (9th Cir. 2003) (“A distinction between removing an item once it has appeared on the Internet and screening before publication cannot fly[].”).

By contrast, the CDA does not bar claims against “information content providers.” An entity “that is responsible, in whole or in part, for the creation or development” of the allegedly offending information is not entitled to the CDA’s protection. “Development” refers “not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness.” Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1167–68 (9th Cir. 2008). Thus, “providing neutral tools to carry out what may be unlawful or illicit searches does not amount to ‘development’ for purposes of the immunity exception.” Id. at 1169. Nor does inoffensive editing for spelling errors, removing obscenity, or trimming for length. However, “a website operator who edits in a manner that contributes to the alleged illegality — such as by removing the word ‘not’ from a user's message reading ‘[Name] did not steal the artwork’ in order to transform an innocent message into a libelous one — is directly involved in the alleged illegality and thus not immune.” Id.

11 Plaintiffs argue that the CDA protects only an interactive computer service’s decision to exclude offensive content.
Prior to the relation of Plaintiff Pirozzi’s action against Apple to the above-captioned Opperman action, Apple moved to dismiss Pirozzi’s claims pursuant to the same provisions of the CDA. Judge Gonzalez Rogers denied Apple’s motion on two bases. First, she found that Pirozzi’s fraud and misrepresentation claims against Apple arising out of Apple’s conduct or failure to disclose were “not predicated solely upon Apple’s approving and distributing Apps via its online App Store.” Pirozzi v. Apple Inc., 913 F. Supp. 2d 840, 849 (N.D. Cal. 2012). Thus, the CDA did not bar those claims. Second, the court held that it was premature to consider the application of the CDA at the pleading stage based on the “scant record” then before the court because “if Apple is responsible for the ‘creation or development of [the] information’ at issue, then Apple functions as an ‘information content provider’ unprotected by the CDA.” Id.

Here, Apple expressly excludes from its CDA argument any application to Plaintiffs’ fraud and misrepresentation claims, in recognition of Judge Gonzalez Rogers’ first conclusion. With respect to her second conclusion, Apple argues that the CAC, which reproduces many of the allegations in Pirozzi and supplements them with others, contains sufficient allegations from which the Court can now conclude that the CDA bars the remainder of Plaintiffs’ claims against Apple. Plaintiffs again maintain that resolution of the CDA issue must await a later stage of the case.

The cases do not describe a one-size-fits all rule for when to apply the CDA. In some cases the applicability of the CDA is “apparent from the face of the complaint”; in others, it is not. Evans v. Hewlett-Packard Co., No. 13-cv-02477-WHA, 2013 WL 5594717, at *3 (N.D. Cal. Oct. 10, 2013) (quoting Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1200 n.5 (N.D. Cal. 2009)). Here, the Court need not await further discovery before addressing Apple’s CDA argument, because the CAC already pleads sufficient conduct to classify Apple as an “information content provider” whose conduct is not protected by the CDA.

For example, Plaintiffs allege that Apple’s “iOS Human Interface Guidelines” encourage data theft. The guidelines are meant to guide developers as they create apps for the App Store. Among the guidelines are several suggestions that do, on their face, appear to encourage the practices Plaintiffs complain of in this case. For example, Apple tells developers, “don’t force
people to give you information you can easily find for yourself, such as their contacts or calendar information,” and “[i]f possible, avoid requiring users to indicate their agreement to your [end user license agreement] when they first start your application. Without an agreement displayed, users can enjoy your application without delay.” CAC ¶ 212 (emphasis omitted). Based on these passages from the guidelines, Plaintiffs allege: “Apple taught Program registrants’ to incorporate forbidden data harvesting functionalities — even for private “contacts” — into their Apps and encouraged Program registrants to design those functions to operate in non-discriminable manners that would not be noticed by the iDevice owner. These App Defendants, apparently in accord with Apple’s instructions, did just that with their identified Apps.” CAC ¶ 214. Similarly, Plaintiffs allege: “Apple’s Program tutorials and developer sites [] teach Program registrants how to code and build apps that non-consensually access, manipulate, alter, use and upload the mobile address books maintained on Apple iDevices.” CAC ¶ 190.

These allegations target conduct that goes beyond the traditional editorial functions of a publisher, and beyond providing “neutral tools to carry out what may be unlawful or illicit” conduct. Apple’s alleged conduct potentially constitutes contribution to the alleged illegality in

12 It is worth noting that not all of Plaintiffs’ allegations concerning Apple’s conduct fall outside the CDA. For example, Plaintiffs’ assertion that Apple “provides third-party developers with review guidelines, and conducts a review of all applications submitted for inclusion in the App Store for compliance with these documents,” CAC ¶ 89, is identical to an allegation regarding the app distributor in Evans, which that court found insufficient to support the plaintiff’s claim that the distributor was also a co-creator. See Evans, 2013 WL 5594717, at *4 (“plaintiffs allege that defendants ‘[m]andated specific “Application Content Criteria” for all content of the App,’ ‘[m]andated “App Naming Guidelines” for the App,’ and ‘[m]andated technical criteria for the App’”).

Apple’s role as an app publisher, including its promulgation of review guidelines, its review of all apps submitted to the App Store, and its enforcement of its guidelines, is fundamental “publisher” activity protected by the CDA. Plaintiffs’ allegations that Apple has failed to remove offending apps from the App Store, CAC ¶ 90, and that it encourages consumers to download third-party apps and advertises third-party apps in order to sell its devices are similarly subject to the CDA’s protections.

Plaintiffs’ allegations concerning the software development kit also fall under the CDA, because the kit is alleged to be nothing more than a “neutral tool” which app developers can use either lawfully or unlawfully. Nothing in the CAC suggests that the kit itself contributes to the practice of taking contact databases without consent. The kit, technologically speaking, makes that
a manner that invokes the “information content provider” exception to the CDA’s protections. See Roommates.Com, 521 F.3d at 1167–68. At this juncture, the Court therefore cannot conclude that Plaintiffs’ theories of liability deriving from Apple’s encouragement of the harvesting of contact information without obtaining consent from the user are not barred by the CDA. See, e.g., Swift v. Zynga Game Network, Inc., No. 09-cv-05443-SBA, 2010 WL 4569889, at *4–6 (N.D. Cal. Nov. 3, 2010) (allegation that video game developer encouraged the creation of and consumption of special offer “scams” were sufficient at pleading stage).

C. Misrepresentation Claims

Apple groups as “misrepresentation claims” Plaintiffs’ UCL, FAL, CLRA, and negligent misrepresentation claims. Apple argues that each claim fails as a matter of law because, according to Apple, “not once in the 166-page pleading does a single Plaintiff identify any specific misrepresentation that he or she actually saw and relied upon in purchasing an Apple device.” ECF No. 395 at 23.

Plaintiffs’ misrepresentation claims are subject to Rule 9(b)’s requirement that fraud claims be pleaded with particularity.13 Plaintiffs’ allegations must therefore include “an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations.” Swartz v. KPMG LLP, 476 F.3d 756, 765 (9th Cir. 2007). The purpose of this requirement is to provide the defendant with adequate notice of the claims against it; plaintiffs must allege “‘what is false or misleading about a statement, and why it is false.’” Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting In re GlenFed, Inc. Sec. Litig., 42 F.3d 1541, 1548 (9th Cir. 1994)).

Plaintiffs must also adequately plead injury and causation. To have standing under the UCL, a plaintiff must have suffered an injury in fact and “lost money or property as a result of practice possible, but it also allows for developers to ask for permission first, rendering the tool “neutral” in nature.

13 Rule 9(b) does not apply to Plaintiffs’ UCL claims for “unlawful” business practices to the extent these claims are grounded on something other than fraud.
such unfair competition.” Hall v. Time Inc., 158 Cal. App. 4th 847, 849 (2008). The standing requirement is substantially similar in this context for Plaintiff’s CLRA and FAL claims. See Kwikset Corp. v. Super. Ct., 51 Cal. 4th 310, 322 (2011) (a plaintiff must “establish a loss or deprivation of money or property sufficient to qualify as injury-in-fact” under the UCL and FAL); Meyer v. Sprint Spectrum L.P., 45 Cal. 4th 634, 646 (2009) (“[I]n order to bring a CLRA action, not only must a consumer be exposed to an unlawful practice, but some kind of damage must result.”). And for negligent misrepresentation claims, a plaintiff must establish detrimental reliance. For all of Plaintiff’s misrepresentation claims, the parties agree that “[w]ithout such reliance, there is no recovery.” Bily v. Arthur Young & Co., 3 Cal. 4th 370, 413 (1992).

Nevertheless, “[w]hile a plaintiff must show that the misrepresentation was an immediate cause of the injury-producing conduct, the plaintiff need not demonstrate it was the only cause.” In re Tobacco II Cases, 46 Cal. 4th 298, 326 (2009). “Moreover, a presumption, or at least an inference, of reliance arises wherever there is a showing that a misrepresentation was material.” Engalla v. Permanente Med. Grp., Inc., 15 Cal. 4th 951, 977 (1997). A misrepresentation is material if a reasonable person “would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question”; materiality is therefore ordinarily a question of fact unless the “fact misrepresented is so obviously unimportant that the jury could not reasonably find that a reasonable man would have been influenced by it.” Id. (quotations and citations omitted).

1. **Specific Representations**

In many consumer fraud cases, courts require a plaintiff to identify and describe the specific alleged misrepresentations that each plaintiff saw or heard, and upon which each plaintiff relied. Indeed, in granting Apple’s first motion to dismiss Plaintiff Pirozzi’s complaint, Judge Gonzalez Rogers held that Pirozzi’s failure to “provide the particulars of her own experience

---

14 Whether a party has Article III standing to bring a cause of action in federal court is a different analysis than whether the plaintiff has adequately established statutory standing under California’s UCL, CLRA, or FAL. Two Jinn, Inc. v. Gov’t Payment Serv., Inc., No. 09-CV-2701-JLS, 2010 WL 1329077, at *3 (S.D. Cal. Apr. 1, 2010).
reviewing or relying upon any” of the misrepresentations identified in her complaint was fatal to her claims. Pirozzi I, 913 F. Supp. 2d at 850. This Court denied Apple’s second motion to dismiss based on Pirozzi’s identification of the specific representations she saw and relied upon, which representations are also alleged here. Pirozzi II, 2013 WL 4029067, at *6–7. Apple now argues that the Court’s prior order was based on a misreading of Pirozzi’s allegations and renews its motion to dismiss.

Having again examined Pirozzi’s allegations, the Court now concludes that its prior decision regarding reliance was in error. In her Second Amended Complaint, Pirozzi alleged that Apple’s website contained the same representations discussed here, including the representation that “[a]ll apps run in a safe environment, so a website or app can’t access data from other apps.”15 Pirozzi II, 2013 WL 4029067, at *7. In its Order, the Court stated: “Plaintiff also alleges that she relied on that statement in making her purchasing decision.” Id. In actuality, however, Pirozzi did not allege that she relied on the statement; rather, she alleged only that she “visited Apple’s website,” not that she read the particular representations she alleged were misleading. Pirozzi v. Apple Inc., No. 12-cv-1529-JST, ECF No. 29 ¶ 10 (filed Jan. 22, 2013). Therefore, Pirozzi’s allegations of reliance were inadequate.

The CAC suffers from the same defect. It repeats the identical allegations made in Pirozzi’s Second Amended Complaint, and repeats the allegation that Pirozzi “viewed the Apple website.” CAC ¶¶ 121–25. In the next paragraph, the CAC further alleges: “Likewise, each of the other Plaintiffs visited Apple’s website . . . .” What the CAC fails to do is connect any specific Plaintiff to any specific representation. The Court now concludes, even reading the complaint in the light most favorable to Plaintiffs, that Plaintiffs have failed to allege that any one of them saw any particular representation.

15 The Court rejects Apple’s argument that this statement is not actionable because it is literally true. The CAC alleges that, although it comes pre-loaded on iDevices, the Contacts app is an app like any other.
2. **Pleading a Long-Term and Extensive Advertising Campaign**

Recognizing that the few specific representations relied upon by this Court in denying Apple’s second motion to dismiss Pirozzi’s complaint form a narrow basis upon which to base this action, Plaintiffs now largely rest their misrepresentation claims on a different basis: that Apple allegedly engaged in a long-standing, widespread advertising campaign that created a reputation for safety and reliability. *In re Tobacco II*, 46 Cal. 4th at 328 (“where, as here, a plaintiff alleges exposure to a long-term advertising campaign, the plaintiff is not required to plead with an unrealistic degree of specificity that the plaintiff relied on particular advertisements or statements”).

The named plaintiffs in *In re Tobacco II* alleged that the tobacco industry defendants conducted “a decades-long campaign of deceptive advertising and misleading statements about the addictive nature of nicotine and the relationship between tobacco use and disease.” *Id.* at 306. In concluding that the plaintiffs did not need to identify the specific statements upon which they relied, the California Supreme Court relied in part on a similar decision in *Whiteley v. Philip Morris Inc.*, 117 Cal. App. 4th 635, 680–82 (2004).

In *Whiteley*, the California Court of Appeal affirmed a jury verdict in favor of the plaintiff, the husband of a woman who was a smoker and died of lung cancer. The tobacco industry defendants argued on appeal that the plaintiff had failed to present sufficient evidence of reliance to support the verdict. In particular, the defendants argued, as Apple does here, “that the evidence did not show that Whiteley heard any *specific* misrepresentation or false promise made by either defendant.” They further argued: “it is not enough that the plaintiff heard the alleged misrepresentation at some unidentified time from some unidentified source. Instead, the plaintiff must identify a *specific* misrepresentation that was *actually communicated* to the plaintiff (directly or indirectly).” *Id.* at 680. The *Whiteley* court expressly rejected that argument and held that the plaintiff “did not have to prove that she saw or heard any specific misrepresentations of fact or false promises that defendants made or that she heard them directly from defendants or their agents. It was sufficient that the statements were issued to the public with the intent that they reach smokers and potential smokers and that Whiteley, as a member of the intended target
population, heard them.” *Id.* at 680–81.

Relying on section 533 of the Restatement Second of Torts, the court held that the trial court had correctly instructed the jury on this question as follows: “One who makes a misrepresentation or false promise or conceals a material fact is subject to liability if he or she intends that the misrepresentation or false promise or concealment of a material fact will be passed on to another person and influence such person's conduct in the transaction involved . . . . One who makes a misrepresentation or false promise or conceals a material fact with the intent to defraud the public or a particular class of persons is deemed to have intended to defraud every individual in that category who is actually misled thereby.” *Id.* at 681. The *Whiteley* court affirmed the jury’s verdict in favor of the plaintiff because the tobacco defendants’ statements were intended to reassure smokers and potential smokers about the health hazards of smoking and to convey that safety message. That was exactly the message Whiteley received. Defendants' and their agents' multifarious misrepresentations regarding the unsettled state of knowledge and the unreliability of any link between cigarette smoking and serious disease were made with the intention and expectation that these misrepresentations would circulate among and influence the conduct of all smokers and prospective smokers. They were heard by or passed on to Whiteley, who believed them.

*Id.* at 681–82.

While several courts have considered whether to apply *Tobacco II* so as to relieve an individual plaintiff of the need to plead that she viewed and relied on a specific misrepresentation, the cases in the aggregate do not define any bright line rules. A review of the jurisprudence, however, has led the Court to identify the following factors in determining whether to apply *Tobacco II*.

First, to state the obvious, a plaintiff must allege that she actually saw or heard the defendant’s advertising campaign. See, e.g., Pfizer Inc. v. Super. Ct., 182 Cal. App. 4th 622, 632 (2010) (“[A]lthough Pfizer ran four different television commercials with the ‘as effective as floss’ campaign, the commercials did not run continuously and there is no evidence that a majority of Listerine consumers viewed any of those commercials.”); Herrington, 2010 WL 3448531, at *8 (“Plaintiffs have not plead that they viewed any of Defendants' advertising, let alone a ‘long-term
advertising campaign’ by Defendants”); Delacruz v. Cytosport, Inc., No. 11-cv-3532-CW, 2012 WL 2563857, at *9 (N.D. Cal. June 28, 2012) (“Cytosport II”) (“Plaintiff has not alleged reliance in connection with the advertising campaign because she has not claimed that she saw and relied on any of the advertising, apart from the product websites and television ads”).

Second, the advertising campaign at issue should be sufficiently lengthy in duration, and widespread in dissemination, that it would be unrealistic to require the plaintiff to plead each misrepresentation she saw and relied upon. Compare Tobacco II, 46 Cal. 4th at 306 (plaintiffs excused from pleading specific reliance where advertising campaign lasted for “decades”); Comm. On Children’s Television, Inc. v. Gen. Foods Corp., 35 Cal. 3d 197, 205–07 (1983) (superseded on other grounds) (advertising campaign was on television daily and lasted four years),16 with In re iPhone 4S, 2013 WL 3829653, at *12 (“The campaign was only about six months old when the CCAC was filed . . . . Plaintiffs have not alleged that the campaign here was comparable to that at issue in Tobacco II’); Delacruz v. Cytosport, Inc., No. 11-cv-3532-CW, 2012 WL 1215243, at *8 (N.D. Cal. Apr. 11, 2012) (“Cytosport I”) (“Plaintiff has failed to allege that Defendant’s advertising campaign approached the longevity and pervasiveness of the marketing at issue in Tobacco II’); Cytosport II, 2012 WL 2563857, at *9 (“The additional allegations regarding the scope of the advertising campaign do not establish that the advertising campaign was as lengthy or pervasive as the tobacco campaign”); In re Yasmin & Yaz (Drospirenone) Mktg., Sales Practices & Products Liab. Litig., No. 09-md-02100-DRH, 2012 WL 865041, at *9 n.20 (S.D. Ill. Mar. 13, 2012) (in class certification context, distinguishing Tobacco II because advertising campaign lasted only eighteen months and involved two advertisements and one corrective advertisement that may have been viewed by class members). How long and how extensive the advertising campaign must be is a fact-intensive inquiry; some campaigns will be too short, such as the six-

16 Children’s Television was decided before Tobacco II, but is included here because it employs a similar analysis. The court there found that in light of defendants’ “large scale program of deceptive advertising in which the specific advertisements change constantly,” it would be impractical to require plaintiffs to plead the specifics of each advertisement. Children’s Television, 35 Cal. 3d at 214.
month campaign in iPhone 4S, and others will be insufficiently extensive, such as the two advertisements in In re Yasmin & Yaz, published over the course of eighteen months.

Third, a plaintiff seeking to take advantage of the exception should describe in the complaint, and preferably attach to it, a “representative sample” of the advertisements at issue in order adequately to notify the defendant of the precise nature of the misrepresentation claim — that is, what, in particular, the defendant is alleged to have said, and how it was misleading. For example, in Children’s Television, 35 Cal. 3d at 205–07, the court held that a trial court “could reasonably require plaintiffs to set out or attach a representative selection of advertisements, to state the misrepresentations made by those advertisements, and to indicate the language or images upon which any implied misrepresentations are based.” Id. at 218. In the California Supreme Court’s view, that requirement “represents a reasonable accommodation between defendants’ right to a pleading sufficiently specific ‘that the court can ascertain for itself if the representations . . . were in fact material, and of an actionable nature,’ and the importance of avoiding pleading requirements so burdensome as to preclude relief in cases involving multiple misrepresentations.” Id. (citation omitted).

Fourth, the degree to which the alleged misrepresentations contained within the advertising campaign are similar to each other, or even identical, is also an important factor.17 For example, in Ticketmaster L.L.C. v. RMG Technologies, No. 07-cv-2534-ABC, 2007 WL 2989504, at *3 (C.D. Cal. Oct. 12, 2007), Ticketmaster alleged that the defendant had marketed and sold an application that enabled customers to violate the Terms of Use and circumvent the security measures on Ticketmaster’s website by purchasing large quantities of tickets. Because the complaint adequately alleged that the defendant aided and abetted its customers’ “same false promise” thousands of times, the court held it was not necessary for the plaintiff to identify “each instance of this alleged fraud, or each and every individual involved.” Instead, it was sufficient to identify “to the extent possible the persons involved . . . and set out a time frame for the repeated misrepresentations.” Id. Although Ticketmaster did not arise in the advertising context, it

17 This does not mean that the representations must be identical. In both Children’s Television and Tobacco II, the advertisements at issue were “similar by category.”
nevertheless provides helpful guidance for the Court in determining the circumstances that may allow a plaintiff to exercise the advertising campaign exception recognized in In re Tobacco II. Indeed, the decision in In re Tobacco II, itself, yields the rule that if a plaintiff alleges a long-term advertising campaign, the advertisements at issue should be similar enough to be considered as part of one campaign, or the delivery of a single message or set of messages, rather than a disparate set of advertising content published in the ordinary course of commerce.

Fifth, in the absence of specific misrepresentations, a complaint subject to Rule 9(b)’s requirements should plead with particularity, and separately, when and how each named plaintiff was exposed to the advertising campaign. It is not sufficient to plead as a group, nor is it sufficient simply to allege general exposure without more detail. The facts in In re Tobacco II contained such detail. So too in Morgan v. AT&T Wireless Servs., Inc., 177 Cal. App. 4th 1235, 1257–58 (2009), where the plaintiffs alleged that when considering purchasing T68i mobile phones from AT&T Wireless, “they each conducted research in which they encountered AT&T advertisements and press releases explaining the advanced features of the T68i and the improvements AT&T was making and was going to make to its GMS/GPRS network.” They also alleged they were exposed to similar representations at the AT&T store when they purchased their phones and service plans, “and that they relied upon their research (including information from the AT&T advertisements and press releases, and the in-store representations) in deciding to purchase the T68i from AT&T.” Id. Within a “relatively short period of time” after purchasing their phones, and despite AT&T’s marketing concerning the upgrades to its network, AT&T performed upgrades on the network that it knew would render the T68i phones “essentially useless.”

AT&T moved to dismiss because the plaintiffs had failed to identify specific misrepresentations. The court held that the allegations supported the plaintiffs’ various misrepresentation claims, including the UCL, CLRA, FAL, and common law fraud, because the plaintiffs were not required, as AT&T asserts, to plead the specific advertisements or representations they relied upon in making their decisions to purchase the T68i . . . . Although the advertising campaign alleged in this case was not as long-term a campaign as the tobacco companies’ campaign discussed in Tobacco II, it is
alleged to have taken place over many months, in several different media, in which AT&T consistently promoted its GMS/GPRS network as reliable, improving, and expanding.

In the context of the common law fraud claim, the court again observed: “where a fraud claim is based upon numerous misrepresentations, such as an advertising campaign that is alleged to be misleading, plaintiffs need not allege the specific advertisements the individual plaintiffs relied upon; it is sufficient for the plaintiff to provide a representative selection of the advertisements or other statements to indicate the language upon which the implied misrepresentations are based.”

The detail the Court requires here ensures that the advertisements at issue are representations that consumers were likely to have viewed, as opposed to representations that were isolated or more narrowly disseminated, such as statements buried on a rarely-viewed webpage, or made on an investor phone conference. Certainly, such representations could be part of an advertising campaign, but the complaint should describe the mechanism of dissemination for all identified representations.

Sixth, the court must be able to determine when a plaintiff made her purchase or otherwise relied in relation to a defendant’s advertising campaign, so as to determine which portion of that campaign is relevant. Representations made prior to purchase are relevant to a plaintiff’s claim; ones made after are not. Consequently, a plaintiff should describe, to the best of her ability, (1) when the product was purchased, (2) the timeframe of the advertisements at issue, and (3) when the plaintiff was exposed to the advertisements.

These factors are merely one court’s attempt to harmonize the developing jurisprudence of false advertising claims. Future decisions from the California state and federal courts may reveal additional factors, or demonstrate that some of those just listed are not helpful. Nevertheless, these are the factors the Court has been able to identify.

Applying them here, the Court finds that Plaintiffs have not adequately alleged a long-term advertising campaign of the kind that would excuse them from pleading specific reliance. Although Plaintiffs allege a long-term advertising campaign, they fail to do so with the level of
detail that has led other courts to allow such claims to proceed.

First, as set forth above, it is not clear that any of the plaintiffs were actually exposed to Apple’s advertising campaign.

Second, although the CAC alleges with sufficient specificity the length of the advertising campaign at issue — it alleges that the campaign began at least by 2008 and continued up through the filing of the CAC — it does not contain sufficient detail concerning the extent of the advertising. It is unclear from the CAC how often the advertisements were published, or in which media. Without more detail, the Court cannot conclude that it would be “unrealistic” to require Plaintiffs to plead with specificity their exposure to each alleged misrepresentation.

Third, and relatedly, Plaintiffs have not attached or described a “representative sample” of the advertisements at issue. Instead of cursory allegations that Apple “repeatedly represented that Apple’s products are safe and secure, and that private information could not be accessed by third-party apps without the user’s express consent,” CAC ¶ 64, Plaintiffs should describe in detail, or attach, advertisements that they contend are typical of the advertising campaign at issue. The Court is mindful that Plaintiffs have identified some specific representations contained on Apple’s website, or made by Apple’s employees, including its former and current CEOs. But it is not enough. After reading the complaint asserted against it, a defendant should be able to understand which advertising is alleged to be misleading, and how it is misleading, so that it may prepare a defense and identify in discovery the remainder of the advertising at issue — and just as importantly, that advertising which is not at issue. It is only through this process that the parties will be able to cabin, and then narrow, the scope of the litigation in succeeding stages. Because Plaintiffs have failed to allege in sufficient detail the nature of the advertisements, the Court finds that the CAC does not adequately notify Apple of the precise nature of the misrepresentation claims asserted against it.

Fourth, because there is insufficient detail with respect to the advertising at issue, the Court cannot conclude that the alleged misrepresentations are sufficiently similar to each other to constitute a single campaign, message, or set of messages susceptible to uniform treatment.

Fifth, Plaintiffs do not separately allege in any detail how they were exposed to Apple’s
advertising campaign. It is not enough merely to allege that Plaintiffs “viewed Apple’s website, saw in-store advertisements, and/or [were] aware of Apple’s representations regarding the safety and security of the iDevices prior to purchasing their own iDevices.” CAC ¶ 126.

Finally, without engaging Apple’s attempts to develop a factual record at the pleading stage, the Court is mindful of the fact that Plaintiffs have not alleged when they purchased their devices, other than to allege they were all purchased prior to February 2012. Consequently, even if Plaintiffs adequately address the other deficiencies in the CAC, it would still be difficult for the Court to conclude that Plaintiffs were exposed to the advertising at issue prior to purchasing their iDevices without more detailed allegations concerning the chronology of events for each Plaintiff in this case.

3. Failure to Disclose

Plaintiffs argue in the alternative that their misrepresentation claims are viable because Apple had an affirmative duty to disclose material facts of which it had exclusive knowledge, i.e., the vulnerability of Plaintiffs’ iDevices to the theft of their address books by third party apps, rendering it unnecessary for Plaintiffs to identify any misrepresentations.

“As the Ninth Circuit has recently cautioned, in the context of product defect claims, ‘California courts have generally rejected a broad duty to disclose.’” Donohue v. Apple, Inc., 871 F. Supp. 2d 913, 925 (N.D. Cal. 2012) (citing Wilson v. Hewlett-Packard Co., 3d 1136, 1141 (9th Cir. 2012). Nondisclosure or concealment constitutes actionable fraud in only four circumstances: “(1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations but also suppresses some material facts.” LiMandri v. Judkins, 52 Cal. App. 4th 326, 336 (1997).

Plaintiffs argue that their non-disclosure claims fit into each of the last three categories. Because the Court has already determined above that Plaintiffs do not adequately identify Apple’s alleged misrepresentations, only the second and third categories are at issue.

But Plaintiffs’ failure to disclose claims have a separate problem: “[a] manufacturer's
duty to consumers is limited to its warranty obligations absent either an affirmative
misrepresentation or a safety issue.”’ Donohue, 871 F. Supp. 2d at 925 (quoting Oestreicher v.
Alienware Corp., 322 F. App’x 489, 493 (9th Cir. 2009)). Here, Plaintiffs fail to allege when
they purchased their iDevices, when the alleged defects arose, what kind of warranty Apple
provided, the terms of the warranty, and the warranty's duration. Consequently, the Court is
unable to conclude whether the alleged defect manifested within the warranty period, and
therefore cannot sustain Plaintiffs’ claims.

Because Plaintiffs have failed to plead with particularity the specific representations upon
which they relied, have failed adequately to plead a long-term and extensive advertising campaign,
and have failed to satisfy the requirements for a pure nondisclosure or concealment claim, the
Court will grant Apple’s motion to dismiss Plaintiffs’ UCL, FAL, CLRA, and negligent
misrepresentation claims, with leave to amend.

D. California Comprehensive Computer Data Access and Fraud Act

The California Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal.
Penal Code § 502, “expand[s] the degree of protection afforded to individuals, businesses, and
governmental agencies from tampering, interference, damage, and unauthorized access to lawfully
created computer data and computer systems.” Id. § 502(a). Every Plaintiff except Pirozzi asserts
a claim against Apple for violation of the CDAFA. The CDAFA imposes liability, inter alia, on
any person who

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network . . . .

18 Once the warranty expires, a manufacturer does not have an affirmative duty to disclose a latent defect unless it poses an “unreasonable safety hazard.” See Donohue, 871 F. Supp. 2d at 926; Wilson, 668 F.3d at 1141–43.
(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

The CDAFA authorizes the owner of the computer “who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) [to] bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.”

Apple moves to dismiss on several grounds. As an initial matter, the Court notes that, to the extent Plaintiffs’ theories of liability under the CDAFA derive from Apple’s “reviewing, editing, and deciding whether to” make available to its users the offending apps, those claims are barred by the Communications Decency Act, as discussed above.

To the extent Plaintiffs assert a CDAFA claim based on Apple’s encouragement of the development of the offending features of the subject apps, those allegations are insufficiently pleaded. Each subsection of the statute Plaintiffs assert incorporates expressly or by reference a requirement that the defendant acted “without permission.” (defining “computer contaminant”). Courts in this district have interpreted “without permission” to mean “in a manner that circumvents technical or code based barriers in place to restrict or bar a user's access.” Other courts in this district have already persuasively rejected this argument. See also In re Google Android Consumer Privacy Litig., No. 11-md-02264-JSW, 2013 WL 1283236, at *12 (N.D. Cal. Mar. 26, 2013); In re iPhone Application Litig. (“iPhone I”), No. 11-md-02250-LHK, 2011 WL 4403963, at *12–13 (N.D. Cal. Sept. 20, 2011).

Plaintiffs argue that their CDAFA claim is viable because they “did not know that the apps contained the malicious code at issue here.” Other courts in this district have already persuasively rejected this argument. See iPhone I, 2011 WL 4403963, at *12 (“On Plaintiffs' own allegations, the iOS and third party apps — which contain the alleged ‘surreptitious
code’ — were all installed or updated voluntarily by Plaintiffs.”); In re Google Android Consumer Privacy Litig., 2013 WL 1283236, at *12 (“Plaintiffs, however, have not included any facts that show — or lead to a reasonable inference — that the tracking codes have been designed in such a way to render ineffective any barriers the Plaintiffs might wish to use to prevent access to their PII.”).

Plaintiffs’ allegations are materially indistinguishable from the allegations in iPhone I and In re Google Android Consumer Privacy. Although Plaintiffs allege they did not grant permission to the apps to copy their address books, there is no suggestion that the apps overcame “technical or code based barriers in place to restrict or bar a user's access.” According to the CAC, the apps in question had open access to Plaintiffs’ address books.19

Plaintiffs’ CDAFA claims against Apple will be dismissed.

E. Strict Products Liability: Design Defect and Failure to Warn

The Opperman Plaintiffs assert design defect and failure to warn strict products liability claims against Apple. “A manufacturer is strictly liable in tort when an article he places on the market, knowing that it is to be used without inspection for defects, proves to have a defect that causes injury to a human being.” Anderson v. Owens-Corning Fiberglas Corp., 53 Cal. 3d 987, 994 (1991) (quoting Greenman v. Yuba Power Products, Inc., 59 Cal. 2d 57, 62 (1963)).

Importantly, “recovery under the doctrine of strict liability is limited solely to ‘physical harm to person or property.’” Jimenez v. Superior Court, 29 Cal. 4th 473, 482 (2002) (quoting Seely v. White Motor Co., 63 Cal. 2d 9, 18 (1965)). “Damages available under strict products liability do not include economic loss, which includes damages for inadequate value, costs of repair and replacement of the defective product or consequent loss of profits — without any claim

19 The Court recognizes there is a split of authority in this district concerning the appropriate scope of the “without permission” language in the CDAFA. Weingand v. Harland Fin. Solutions, Inc., No. 11-cv-3109-EMC, 2012 WL 2327660, at *5 (N.D. Cal. June 19, 2012). Even Weingand, however, still requires that Defendants have circumvented “restrictions on access” of some kind. The CAC does not allege that the subject apps circumvented any restrictions at all. Instead, it alleges that Apple failed to implement any such restriction, thereby enabling the App Defendants to copy Plaintiffs’ address books. Under either approach to the CDAFA, Plaintiffs fail to state a viable claim.
of personal injury or damages to other property”  Id.  (quotation marks and citations omitted).  By contrast, “[t]he law of contractual warranty governs damage to the product itself.”  Id. at 483.

Plaintiffs do not explain what injury they allege that satisfies the economic loss rule.  The CAC alleges only that “Plaintiffs suffered personal injuries as a result of the defective design, including invasions of their privacy and damages to their properties (the mobile address books).”  CAC ¶ 694.  Those injuries are not “physical harm to person or property” and cannot support a products liability claim.  For this reason, the Court will dismiss Plaintiffs’ strict products liability claim.

F. Negligence

Plaintiffs' negligence claims are barred by the economic loss rule discussed in the immediately previous section.  "Purely economic damages to a plaintiff which stem from disappointed expectations from a commercial transaction must be addressed through contract law; negligence is not a viable cause of action for such claims.”  iPhone II, 844 F. Supp. 2d at 1064.

The Court will dismiss Plaintiffs’ negligence claim against all Defendants.

G. RICO

Plaintiffs state that they “elect not to prosecute [the RICO] claim at this time and have no objection to its dismissal without prejudice as to” Apple.  ECF No. 421 at 50.  The Court construes Plaintiffs’ statement as a Rule 41(a)(1)(A)(i) notice of voluntary dismissal, which is self-executing.

H. Aiding and Abetting

In response to Apple’s argument that aiding and abetting is not a stand-alone cause of action in California, Plaintiffs respond: “The fact that Plaintiffs’ aiding and abetting allegations are set out in a separate claim merely provides clarity to the complaint by specifying that Plaintiffs contend that Apple is liable not just for its own actions but for those of the App Defendants.”  ECF No. 421 at 49.  Far from providing clarity, the separate aiding and abetting count casts in doubt which claims that, facially, are asserted only against the App Defendants are also meant to apply to Apple as well.  The Court cannot discern from the CAC what additional liability, other than the claims Plaintiffs explicitly assert against Apple, Plaintiffs attempt to impose on Apple by virtue of
the aiding and abetting count. For this reason, the Court will dismiss the claim. Plaintiffs are advised that each claim in the complaint should clearly set forth against which Defendants it is meant to be asserted.

IV. APP DEFENDANTS’ MOTIONS TO DISMISS

Like Apple, the App Defendants move to dismiss all of Plaintiffs’ claims against them on Article III standing grounds, as well as pursuant to Rule 12(b)(6).

A. Article III Standing

The Article III standing analysis as applied to Plaintiffs’ claims against the App Defendants differs from the analysis regarding Plaintiffs’ claims against Apple. In particular, the App Defendants argue that Plaintiffs have failed to identify an injury-in-fact sufficient to establish standing.

In evaluating Path’s motion to dismiss the Hernandez complaint prior to the relation of that action to the above-captioned action, Judge Gonzalez Rogers evaluated the alleged injury of “diminished mobile device resources, such as storage, battery life, and bandwidth.” Hernandez v. Path, Inc., No. 12-cv-01515-YGR, 2012 WL 5194120, at *1–2 (N.D. Cal. Oct. 19, 2012). She found that the diminished mobile device resources injury was de minimis. Id. The allegations in the CAC provide no further detail concerning this alleged injury, but instead recast it similar terms. See, e.g., CAC ¶ 147 (“For instance, the unauthorized transmissions and operations used iDevice resources, battery life, energy and cellular time at a cost to Plaintiffs and caused loss of use and enjoyment of some portion of each iDevice’s useful life.”). There is no indication, for example, that battery resources were depleted as in iPhone II. Because Plaintiffs have not quantified or otherwise articulated the alleged resource usage, they fail to allege an injury that can serve as the basis of standing. See, e.g., In re Google, Inc. Privacy Policy Litig., No. 12-cv-01382-

20 The App Defendants also repeat some of the arguments Apple makes, for example that those Plaintiffs who are not from California cannot sue under California law. See ECF No. 393 at 7. Where the Court has already addressed an identical argument in the section on Apple's motion to dismiss, it does not do so again here.

21 Judge Gonzalez Rogers also evaluated two other types of alleged injury that Plaintiffs no longer allege and that are not germane to this Order.
PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) (distinguishing Hernandez because resource usage was significant and “systemic rather than episodic”).

In addition, however, Plaintiffs present four new theories of injury-in-fact not present in Hernandez. First, Plaintiffs argue that their claim for injunctive relief is sufficient to confer standing. “To have standing to assert a claim for prospective injunctive relief, a plaintiff must demonstrate ‘that he is realistically threatened by a repetition of [the violation].’” Melendres v. Arpaio, 695 F.3d 990, 997 (9th Cir. 2012) (quoting City of Los Angeles v. Lyons, 461 U.S. 95, 109 (1983)). Here, Plaintiffs allege that the App Defendants all discontinued their practices when the practice of transmitting user address books was made public. Moreover, Plaintiffs allege that Apple has instituted additional privacy controls that enable users to control which apps have access to their address books. Because there is no realistic threat of repetition, Plaintiffs cannot establish standing through their prayer for injunctive relief.

Second, Plaintiffs argue that the App Defendants interfered with their property rights in their address books, conferring standing on Plaintiffs to sue. “[D]istrict courts have been reluctant to find standing based solely on a theory that the value of a plaintiff’s [personal information] has been diminished.” Yunker v. Pandora Media, Inc., No. 11-cv-03113-JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013). “[I]njury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff’s personal identification information. Rather, a plaintiff must allege how the defendant’s use of the information deprived the plaintiff of the information’s economic value. Put another way, a plaintiff must do more than point to the dollars in a defendant’s pocket; he must sufficiently allege that in the process he lost dollars of his own.” In re Google, Inc. Privacy Policy Litig., 2013 WL 6248499, at *5. See also In re Google Android Consumer Privacy Litig., 2013 WL 1283236, at *4 (“Similarly, although Plaintiffs allege that a market exists that could provide them the opportunity to sell their PII, none of the Plaintiffs specifically tie those allegations to them. Plaintiffs also do not allege they attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from entering into a value for value transaction relating to their PII, as a result of the Google
Defendants' conduct.”). 22

Plaintiffs here have failed to allege any details concerning their argument that their address books’ value was diminished by the App Defendants’ conduct. Instead, Plaintiffs argue that address books are distinct from the “automatically-generated computer data sets” at issue in the multitude of cases in which courts have found allegations similar to Plaintiffs insufficient. The distinction is one without a difference. Whether automatically-generated or generated by the user, Plaintiffs must “tie” their allegations that their personal information has value to the alleged injury they suffered. Here, Plaintiffs have failed to do so. Consequently, Plaintiffs do not have Article III standing based on injury to their property rights.

However, Plaintiffs’ two remaining theories of injury are sufficient to confer standing. First, as observed above, Plaintiffs are able to establish standing through their statutory claims, because “[t]he injury required by Article III can exist solely by virtue of ‘statutes creating legal rights, the invasion of which creates standing.’” Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010) (quoting Fulfillment Servs. Inc. v. United Parcel Serv., Inc., 528 F.3d 614, 618 (9th Cir. 2008)). See In re Google, Inc. Privacy Policy Litig., 2013 WL 6248499, at *8 (“Although Article III always requires an injury, the alleged violation of a statutory right that does not otherwise require a showing of damages is an injury sufficient to establish Article III standing.”).

Second, Plaintiffs assert a common law claim for invasion of privacy. Regardless of the merits of that claim, the Court finds Plaintiffs’ allegations sufficient on this point. The essence of the standing inquiry is to determine whether the plaintiff has “alleged such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends.” Baker v. Carr, 369 U.S. 186, 204 (1962). It is

22 The Court does not read these decisions to be holding that consumers do not have property rights in their electronically stored private information, but that the copying of such information without any meaningful economic injury to consumers is insufficient to establish standing on that basis. Cf. FMC Corp. v. Capital Cities/ABC, Inc., 915 F.2d 300, 303–04 (7th Cir. 1990) (applying California law; noting that “[i]n cases where the alleged converter has only a copy of the owner's property and the owner still possesses the property itself, the owner is in no way being deprived of the use of his property. The only rub is that someone else is using it as well.”).
beyond meaningful dispute that a plaintiff alleging invasion of privacy as Plaintiffs do here presents a dispute the Court is permitted to adjudicate. See, e.g., Wright & Miller, 13A Fed. Prac. & Proc. Juris. § 3531.4 (3d ed.); Ruiz v. Gap, Inc., 380 F. App’x 689, 691 (9th Cir. 2010) (unpublished) (holding allegation that laptop theft put plaintiff at “greater risk of identity theft” was sufficient injury, even where plaintiff had no UCL standing); Yunker, 2013 WL 1282980, at *6 (finding Article III standing based on violation of constitutional privacy rights); Citizens for Health v. Leavitt, 428 F.3d 167, 176 & n.9 (3d Cir. 2005), cert. den’d 127 S. Ct. 43 (2006) (holding Plaintiffs had standing to challenge “Privacy Rule” that allowed medical providers to use or disclose personal health information without patient consent because summary judgment evidence showed “at least one individual plaintiff’s health information has been, or will imminently be, disclosed without her consent by private health care providers and drugstore chains”); Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 990 (2011) (discussing invasion of privacy claims). The App Defendants do not respond to this theory of injury. The Court finds it is sufficient to confer standing for those claims on which the injury bears — intrusion upon seclusion and public disclosure of private facts.

For the foregoing reasons, the Court will dismiss Plaintiffs’ common law claims against the App Defendants, except their invasion of privacy claims, on standing grounds.

B. Plaintiffs’ UCL Claims

The Court will also dismiss Plaintiffs’ UCL claims against the App Defendants, because, in order to have standing to assert their UCL claims, Plaintiffs must show that they “lost money or property,” and, as the Court concludes above, they have failed to make such a showing. See Kwikset Corp. v. Super. Ct., 51 Cal. 4th 310, 325 (2011).

C. Invasion of Privacy: Intrusion Upon Seclusion

The Opperman Plaintiffs assert the common law claim of intrusion upon seclusion against the App Defendants. In particular, Plaintiffs allege that “[b]y surreptitiously obtaining, improperly gaining knowledge, reviewing and retaining Plaintiffs’ private mobile address books (or substantial portions thereof), the App Defendants intentionally intruded on and into each respective Plaintiff’s solitude, seclusion or private affairs.” CAC ¶ 630. Plaintiffs allege the
intrusion was “highly offensive to a reasonable person,” as evidenced by the “myriad newspaper articles, blogs, op eds., and investigative exposes’ [that] were written complaining and objecting vehemently to these defendants’ practices.” CAC ¶ 631. Plaintiffs also allege that “[c]ongressional inquiries were opened to investigate these practices and some defendants even publicly apologized. The surreptitious manner in which the App Defendants’ conducted these intrusions confirms their outrageous nature.” Id.

The Second Restatement of Torts provides: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” Rest. (2d) of Torts § 652B (1977). California courts recognize that “a measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by these concepts.” Shulman v. Grp. W Prods., Inc., 18 Cal. 4th 200, 231 (1998) (quoting Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L.Rev. 962, 973–974 (1964) (footnote omitted)).

An intrusion upon seclusion claim “does not depend upon any publicity given to the person whose interest is invaded or to his affairs.” Rest. (2d) of Torts § 652B, Comment a. Nor must the intrusion be physical:

it may be performed by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.

Id., Comment b. California has adopted the Restatement’s two-prong formulation of intrusion upon seclusion claims: “(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person.” Shulman, 18 Cal. 4th at 231.
“The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.”  Id. Whether a legally protected privacy interest is at stake is a question of law; whether a plaintiff has a reasonable expectation of privacy and whether the defendant’s conduct is a serious invasion of privacy are mixed questions of law and fact. See Hill v. Nat’l Collegiate Athletic Assn., 7 Cal. 4th 1, 39–40 (1994) (discussing California constitutional invasion of privacy). “If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law.”  Id.

The Court does not read the App Defendants to be contesting that Plaintiffs have a legally protectable privacy interest in their address books, nor do the App Defendants contest that the apps intruded upon that interest. Instead, the App Defendants argue that Plaintiffs did not have a reasonable expectation of privacy in the information, and that the intrusion was not sufficiently offensive to give rise to a claim for intrusion upon seclusion.

1. Reasonable Expectation of Privacy

A claim for intrusion upon seclusion is not viable unless the plaintiff had an “objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.” Shulman, 18 Cal. 4th at 231. Several factors affect a person’s reasonable expectation of privacy. Advance notice of an impending action, customs, practices, and physical settings may “create or inhibit reasonable expectations of privacy.” Hill, 7 Cal. 4th at 36. “Finally, the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant.” Id.

Here, there are two types of alleged intrusions at issue. Plaintiffs allege that some apps copied Plaintiffs’ address books without consent or any prompt. The Court finds that Plaintiffs’ expectation of privacy in their address books contained on their iDevices in this circumstance was reasonable. See, e.g., United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (“[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. Zavala had a reasonable expectation of privacy regarding this information.”); United States v. Cerna, No. 08-cv-0730-WHA, 2010 WL 5387694, at *6 (N.D. Cal. 2010).
Cal. Dec. 22, 2010) (citing Zavala) (“Luis Herrera had a reasonable expectation of privacy in the contents of the seized phones as his physical possession of the cell phones created a reasonable expectation of privacy in their contents.”); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (criminal defendant had expectation of privacy in contents of pager because “[t]he expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information”).

Other apps, such as Gowalla and Instagram, copied address books only after they prompted the user to “find friends” who use the same app by scanning Plaintiffs’ address books. See, e.g., CAC ¶¶ 238, 317. The menu prompts notified users that the app would scan their address books. Although the prompts required Plaintiffs to consent, Plaintiffs’ expectation of privacy in that circumstance was still reasonable. Plaintiffs allege that they would not have consented had they known that their apps would not only scan their address books to determine whether their friends were using the same app, but then upload the address books to the app developer for other purposes. Plaintiffs allege that their consent was obtained by fraud, and that their consent was therefore invalid. See Rest. (2d) of Torts § 892B (1979) (“If the person consenting to the conduct of another is induced to consent by a substantial mistake concerning the nature of the invasion of his interests or the extent of the harm to be expected from it and the mistake is known to the other or is induced by the other's misrepresentation, the consent is not effective for the unexpected invasion or harm.”); Sanchez-Scott v. Alza Pharm., 86 Cal. App. 4th 365, 377–78 (2001) (sustaining intrusion upon seclusion claim where doctor obtained consent of patient to breast examination in front of a drug salesperson without disclosing salesperson was not a medical professional).

Here, Plaintiffs allege that the App Defendants obtained their consent by misrepresenting their purpose. That is, they allege that the App Defendants intentionally represented that they would only “scan” Plaintiffs’ address books for purposes of the “find friends” feature without disclosing that, at the same time, the app would transmit a copy of the address book to Defendants for their own use. Taking the allegations in the CAC as true, the Court concludes that Plaintiffs’ consent was invalid. Consequently, Plaintiffs had a reasonable expectation of privacy with respect
to the address books copied by each app at issue.

2. Offensiveness

The App Defendants’ primary argument in support of their motion to dismiss Plaintiffs’ intrusion upon seclusion claim is that the intrusion at issue is not “highly offensive.”

Liability for intrusion upon seclusion will not lie “unless the interference with the plaintiff’s seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.” Rest. (2d) of Torts § 652B, Comment d. “A court determining the existence of ‘offensiveness’ would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.” Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1483–84 (1986).

In evaluating a claim for invasion of California’s constitutional right to privacy, the iPhone II court held that the surreptitious tracking of personal data and geolocation information was not an “egregious breach of social norms.” 844 F. Supp. 2d at 1063. In coming to that conclusion, that court relied primarily on the decision in Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 992 (2011). In Folgelstrom, the plaintiff alleged that the defendant retailer routinely asked for customers’ zip codes, asked a credit agency to match their zip codes and credit card numbers to home mailing addresses, and then engaged in mail marketing using the addresses. The court first concluded that the plaintiffs did not have a legally protected private interest in their mailing addresses. The court also held that the retailer’s conduct was not egregious, but “routine commercial behavior.” Id. at 992.

The decision in Folgelstrom is distinguishable.23 Here, Plaintiffs allege the theft of the

23 The App Defendants also argue that Folgelstrom limited intrusion upon seclusion claims to conduct that involves a highly offensive use of the private information. See Folgelstrom, 195 Cal. App. 4th at 993 (“[W]e have found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiff’s private information which did not also allege that the use of plaintiff's information was highly offensive.”).

That passage from Folgelstrom is dicta, and the Court has been unable to locate any other decision
information in their personal contact lists, which is more private than a person’s mailing address. And while the Court recognizes that attitudes toward privacy are evolving in the age of the Internet, smartphones, and social networks, the Court does not believe that the surreptitious theft of personal contact information — which is what the CAC alleges — has come to be qualified as “routine commercial behavior.” Indeed, Plaintiffs allege that consumers, the media, the Federal Trade Commission, and Congress have closely scrutinized the practices at issue in this case because of concerns that the practices were inappropriate.

The Court cannot conclude as a matter of law that Defendants’ copying of Plaintiffs’ address books was not “highly offensive.” That question is best left for a jury.

3. **Damages**

The App Defendants briefly argue that Plaintiffs have failed adequately to allege damages from the alleged intrusion upon seclusion because they have failed to allege economic injury. No such allegation is required. A plaintiff who prevails on an intrusion upon seclusion claim may recover damages for “anxiety, embarrassment, humiliation, shame, depression, feelings of powerlessness, anguish, etc.” Operating Engineers Local 3 v. Johnson, 110 Cal. App. 4th 180, 187 (2003) (quoting Miller v. National Broadcasting Co., 187 Cal. App. 3d 1463, 1485 (1986)).

For the foregoing reasons, the Court will deny the App Defendants’ motion to dismiss the Opperman Plaintiffs’ claim for intrusion upon seclusion.

that has applied the limitation; it was not relied upon, for example, in iPhone II. Moreover, unlike the Folgelstrom court, this Court has been able to locate cases which impose liability without an allegation of highly offensive use. For example, in Sanchez-Scott v. Alza Pharm., 86 Cal. App. 4th 365, 377–78 (2001), a patient adequately stated an intrusion upon seclusion claim where her doctor performed a breast examination in front of a pharmaceutical salesperson without revealing that the salesperson was not a medical professional. In that case, no “highly offensive use” was at issue, only the highly offensive manner in which the privacy interest was invaded.

The Restatement also expressly disavows any such limitation. See Rest. (2d) of Torts § 652B, Comment b (“The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.”) (emphasis added).
D. Invasion of Privacy: Public Disclosure of Private Facts

The Opperman Plaintiffs also assert an invasion of privacy claim for public disclosure of private facts.

The elements of a claim for public disclosure of private facts are: “(1) public disclosure, (2) of a private fact, (3) which would be offensive and objectionable to the reasonable person, and (4) which is not of legitimate public concern.” Taus v. Loftus, 40 Cal. 4th 683, 717 (2007) (quotation omitted). Here, Plaintiffs have failed to allege a public disclosure.

The Restatement makes clear that Plaintiffs must allege disclosure to the public “at large”:

“Publicity,” as it is used in this Section, differs from “publication,” as that term is used in § 577 in connection with liability for defamation. “Publication,” in that sense, is a word of art, which includes any communication by the defendant to a third person. “Publicity,” on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. The difference is not one of the means of communication, which may be oral, written or by any other means. It is one of a communication that reaches, or is sure to reach, the public.

Thus it is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons. On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity within the meaning of the term as it is used in this Section. The distinction, in other words, is one between private and public communication.

Rest. (2d) of Torts § 652D, Comment a (1977).

Plaintiffs argue that they satisfy this standard because their address books were transmitted in an unencrypted manner, or over public WiFi, “making it publicly available to third parties as well as service providers.” ECF No. 422 at 27. That argument fails to meet the disclosure requirement for this claim. While Plaintiffs allege that their information could have been intercepted by third parties, they do not allege that any interception occurred, nor do they allege that it was “substantially certain” that their address books would become “public knowledge.” To
satisfy the requirement, more specific allegations establishing the extent of the disclosure are required.

For this reason, the Court will dismiss the Opperman Plaintiffs’ public disclosure claim.

E. CDAFA and Computer Fraud and Abuse Act

The Court’s analysis supra, Part III.D, concerning the California Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502, applies equally to Plaintiffs’ claims against the App Defendants. For the challenged conduct to qualify as “without permission” under the CDAFA, the conduct must involve circumventing “restrictions on access” of some kind. The CAC does not allege that the subject apps circumvented any restrictions.

Plaintiffs also assert a claim for violation of the federal Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. §§ 1030(a)(2)(C), (a)(5), & (g), against the App Defendants. Plaintiffs concede that, like the CDAFA, the CFAA applies only to a defendant’s access to a computer “without authorization,” and that this limitation must be interpreted similarly to the “without permission” language in the CDAFA. See, e.g., iPhone I, 2011 WL 4403963, at *11 (“Where the software that allegedly harmed the phone was voluntarily downloaded by the user, other courts in this District and elsewhere have reasoned that users would have serious difficulty pleading a CFAA violation.”).

Plaintiffs do not advance any new arguments concerning the “without authorization” limitation in the CFAA, relying instead on their arguments concerning the CDAFA. Consequently, the Court will dismiss both claims.

F. Electronic Communications Privacy Act

The Federal Wiretap Act, or Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2510, prohibits “interception” of “wire, oral, or electronic communications.” Id. § 2511(1). The Act provides a private right of action against any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication,” id. § 2511(1)(a), or who “intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication
in violation of [the Wiretap Act].” \textit{id.} § 2511(1)(d). “\textit{Intercept}” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” \textit{id.} § 2510.

All Plaintiffs except Pirozzi assert an ECPA claim against the App Defendants. Judge Gonzalez Rogers previously dismissed the ECPA claim in \textit{Hernandez} for the same reason the App Defendants seeks dismissal here: “The FAC fails to allege that Defendant intercepted any communication contemporaneously with its transmission. Although Path allegedly transmitted the Class Members’ Contact Address Books from the Class Members’ mobile devices to Path’s servers, Path did not ‘intercept’ a ‘communication’ to do so.” \textit{Hernandez}, 2012 WL 5194120, at *3.

Similarly, the Ninth Circuit has noted that “\textit{interception}” means “‘\textit{communication contemporaneous with transmission}.’” \textit{Theofel v. Farey-Jones}, 359 F.3d 1066, 1077 (9th Cir. 2004) (quoting \textit{Konop v. Hawaiian Airlines, Inc.}, 302 F.3d 868, 876 (9th Cir. 2002) (holding unauthorized access to e-mail messages did not violate ECPA). “Specifically, Congress did not intend for ‘\textit{intercept}’ to apply to ‘\textit{electronic communications}’ when those communications are in ‘\textit{electronic storage}.’” \textit{id.} (internal quotation marks omitted) (quoting \textit{Konop}, 302 F.3d at 876).

Plaintiffs simultaneously “preserv[e] their disagreement with this court-generated rule in the event it is later overturned,” ECF No. 422 at 24, and also advance the tortured argument that the contemporaneous interception requirement is met here because the apps in question caused Plaintiffs’ iDevices to “send information from the user’s Contacts from the iDevice’s storage memory to processors and active memory being used by the app” and then “simultaneously intercept[ed] that transmission.” \textit{id.} The decisions in \textit{Konop} and \textit{Theofel} are dispositive. In those cases, the “\textit{transmission}” Plaintiffs describe here as being “\textit{intercepted}” —the use of data by different memory components of the same device — was insufficient to give rise to an ECPA claim. The Court will dismiss Plaintiffs’ ECPA claim.

\textbf{G. Texas and California Wiretap Statutes}

Plaintiffs incorporate by reference their arguments concerning the ECPA with respect to those claims, and do not present any other argument concerning the “interception” requirement in the Texas and California statutes. The Court will dismiss those claims for the same reasons. See, e.g., Hernandez, 2012 WL 5194120, at *5.

H. Texas Theft Liability Act

The Texas Plaintiffs assert a claim for violation of Texas Penal Code section 31.03(a), which provides that a person commits theft: “if he unlawfully appropriates property with intent to deplete the owner of property.” “Deplete” means “(A) to withhold property from the owner permanently or for so extended a period of time that a major portion of the value or enjoyment of the property is lost to the owner; (B) to restore property only upon payment of reward or other compensation; or (C) to dispose of property in a manner that makes recovery of the property by the owner unlikely.” Tex. Pen. Code § 31.01(2)(A)–(C).

Plaintiffs cannot satisfy the definition of “deplete” for purposes of their Texas Theft Liability Act claim. Even if Plaintiffs have a property right in their address books, there is no allegation that the App Defendants withheld the address books from Plaintiffs “permanently or for so extended a period of time that a major portion of the value or enjoyment of the property” was lost. Nor do Plaintiffs allege that the App Defendants offered to restore the address books for payment, because no restoration is possible; the address books were copied. For the same reason, Plaintiffs have not alleged that the App Defendants disposed of the property. Consequently, the Court will dismiss the Texas Plaintiffs’ Texas Theft Liability Act claim.

I. RICO and Vicarious Liability

Plaintiffs “elect not to prosecute [their RICO and vicarious liability] claims at this time and have no objection to their dismissal without prejudice as to” the App Defendants. As discussed above with respect to Plaintiffs’ RICO claim against Apple, the Court construes Plaintiffs’ statement as a Rule 41(a)(1)(A)(i) notice of voluntary dismissal, which is self-executing.

V. Facebook and Gowalla’s Motion to Dismiss

App Defendants Facebook and Gowalla move to dismiss Plaintiffs’ claims against them for violation of the Uniform Fraudulent Transfer Act (“UFTA”), Cal. Civ. Code § 3439, et seq.,
for common law aiding and abetting, and for successor liability (as against Facebook only).

Plaintiffs allege that “[i]n late 2011, Facebook conducted due diligence on Gowalla for a contemplated business transaction with Gowalla and/or Gowalla’s owners. The contemplated transaction involved transfer of all or substantially all of Gowalla’s assets, technology, know-how or equity to Facebook.” CAC ¶ 414. According to the CAC, Facebook discovered that Gowalla’s app had been copying users’ address books without consent and decided as a result to structure the transaction differently. The resulting transaction transferred to Facebook Gowalla’s key personnel, “technology” and “know-how.” CAC ¶ 416. “Facebook did not pay Gowalla reasonably fair value for the Gowalla assets, technology, know-how or personnel. Facebook instead paid Gowalla’s shareholders and management for the company’s assets. On information and belief, Facebook made payments of cash and/or Facebook pre-IPO stock to Gowalla’s stockholders and management (instead of Gowalla) in consideration for this transaction.” CAC ¶ 417. The transaction left Gowalla “effectively headless, lacking independent (or any) continuing management, and insolvent” CAC ¶ 418.

The transaction was memorialized in a Release and Waiver Agreement submitted to the Court under seal by Facebook and Gowalla. The Agreement demonstrates that Facebook transferred a substantial amount of cash and pre-IPO shares to Gowalla, not to Gowalla’s shareholders or owners. The Agreement also conveyed to Facebook a non-exclusive, royalty-free license to Gowalla’s patents. It did not convey title to any of Gowalla’s intellectual property. Finally, the Agreement permitted Gowalla to redistribute the shares Gowalla received under certain conditions. Plaintiffs point out that the Agreement refers to several documents that are not in the record, and that the Agreement does not provide the Court with any information concerning how the contract was performed.

A. Uniform Fraudulent Transfer Act

“The [California] UFTA permits defrauded creditors to reach property in the hands of a

24 Because the CAC depends on the transaction at issue, the Court hereby takes judicial notice of the Agreement. See Swartz v. KPMG, LLP, 476 F.3d 756, 763 (9th Cir. 2007).

Under the California UFTA, a fraudulent transfer may be "actual" or "constructive." Cal. Civ. Code § 3439.04(a). “In order for a fraudulent transfer to occur, among other things, there must be a transfer of an asset as defined in the UFTA.” Schroeder, 179 Cal. App. 4th at 841 (emphasis in original). Under the Act, “transfer” is defined as “every mode, direct or indirect, absolute or conditional, voluntary or involuntary, of disposing of or parting with an asset or an interest in an asset, and includes payment of money, release, lease, and creation of a lien or other encumbrance.” Cal. Civ. Code § 3439.01(i). An “asset” is, in turn, defined by the term “property,” which is defined as “anything that may be the subject of ownership.” Cal. Civ. Code § 3439.01(a), (h). A creditor cannot premise a UFTA claim on a transfer unless the “the transfer puts beyond [the creditor’s] reach property [the creditor] otherwise would be able to subject to the payment of [] debt.” Mehrtash v. Mehrtash, 93 Cal. App. 4th 75, 80 (2001).


Facebook and Gowalla argue that Plaintiffs do not have standing to assert a California UFTA claim against them because they are not residents of California. The Court has already rejected that argument with respect to Apple’s motion to dismiss. Plaintiffs have standing to assert a California UFTA claim against Facebook and Gowalla, which are headquartered in California, for conduct that occurred in California.

As for the choice-of-law analysis, the parties agree that the California and Texas UFTA statutes do not conflict. Consequently, the Court will analyze California’s UFTA.
Here, Plaintiffs’ allegations do not establish that any transfer of assets occurred within the meaning of the UFTA. Plaintiffs only describe generally what assets they assert were transferred: personnel, “technology,” and “know-how.” Plaintiffs fail to address the requirement that the transfer at issue put beyond Plaintiffs’ reach property they otherwise would be able to subject to the payment of debt. There is no suggestion, for example, that Plaintiffs could not subject Gowalla’s intellectual property, which Gowalla retained, to the payment of a future debt, or that the license Gowalla conveyed to Facebook somehow impaired its ability to satisfy creditor claims. Certainly Gowalla’s employees are not “assets” for purposes of the UFTA. The parties have cited only one case to the Court on this point, Fink v. Advanced Logic Sys., Inc., A-5939-05T1, 2007 WL 3239222, at *7 (N.J. Super. Ct. App. Div. Nov. 5, 2007), and there, the court held that a non-exclusive license to copyrighted work was not an asset for purposes of a New Jersey fraudulent transfer. 26

Because Plaintiffs have failed to allege a transfer of assets within the meaning of the UFTA, their UFTA claim will be dismissed.

B. Successor Liability

Each claim asserted against Gowalla in this case is also asserted against Facebook by virtue of successor liability. Under California law, a corporation that purchases the assets of another does not assume the liabilities of the selling corporation unless: “(1) there is an express or implied agreement of assumption, (2) the transaction amounts to a consolidation or merger of the two corporations, (3) the purchasing corporation is a mere continuation of the seller, or (4) the transfer of assets to the purchaser is for the fraudulent purpose of escaping liability for the seller's debts.” Ray v. Alad Corp., 19 Cal. 3d 22, 28 (1977). Plaintiffs’ allegations on this point are materially deficient because they have not alleged that Facebook acquired Gowalla, and, as discussed above, they have failed to allege a transfer of assets. Indeed, the CAC expressly alleges the opposite: that Facebook acquired employees and intellectual property rights, but not Gowalla

26 In briefing and at oral argument, Plaintiffs point to a Facebook securities filing and make other arguments based on facts not contained in the CAC. The Court declines to consider these arguments.
itself.

There is no successor liability where no acquisition or fraudulent transfer has occurred. See, e.g., Gee v. Tenneco, Inc., 615 F.2d 857, 862 (9th Cir. 1980) (“It is the general rule that where a corporation is not dissolved following a sale of assets or a reorganization, it remains liable for debts and liabilities incurred by it, unless it is otherwise agreed between the corporation and its creditors.”). Consequently, Plaintiffs have failed to plead any claims against Facebook by virtue of successor liability.

C. Aiding and Abetting

Facebook argues, and Plaintiffs do not contest, that Texas law applies to Plaintiffs’ claims against it. ECF No. 394 at 6 n.6; ECF No. 434 at 2. Texas does not recognize a claim for “aiding and abetting” as alleged in the CAC.

In Juhl v. Airington, 936 S.W.2d 640, 643 (Tex. 1996), the Texas Supreme Court declined to adopt section 876 of the Restatement (Second) of Torts, which sets out a “concerted action” theory of liability, noting that whether concerted action liability is recognized in Texas would remain an “open question.” No subsequent case, however, has ever allowed such a claim. See Eckhardt v. Qualitest Pharm. Inc., 858 F. Supp. 2d 792, 802 (S.D. Tex. 2012) (“It is an ‘open

27 Section 876 of the Restatement provides:

For harm resulting to a third person from the tortious conduct of another, one is subject to liability if he

(a) does a tortious act in concert with the other or pursuant to a common design with him, or

(b) knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other so to conduct himself, or

(c) gives substantial assistance to the other in accomplishing a tortious result and his own conduct, separately considered, constitutes a breach of duty to the third person.

Rest. (2d) of Torts, § 876 (1977).
question’ whether Texas law would even allow liability to be imposed based on § 876, and
Plaintiffs have not directed the Court to any Texas cases holding a defendant liable under § 876. It
is not the role of this Court, ‘Erie-bound,’ to expand Texas tort law.”).28

Plaintiffs’ aiding and abetting claim will be dismissed.

VI. CONCLUSION

For the foregoing reasons, the Court hereby DISMISSES all of Plaintiffs’ claims against
all Defendants with leave to amend, with the exception of the Opperman Plaintiffs’ claim for
common law intrusion upon seclusion against the App Defendants. Plaintiffs have leave to file an
amended complaint within thirty days from the date of this Order.

IT IS SO ORDERED.

Dated: May 14, 2014

JON S. TIGAR
United States District Judge

28 Plaintiffs argue that because there is no case expressly prohibiting such a claim, Facebook’s
motion to dismiss should be denied. This California federal court will decline Plaintiffs’ invitation
to create new causes of action under the state law of Texas.
CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
SECOND APPELLATE DISTRICT
DIVISION ONE

DIGITAL MUSIC NEWS LLC,

Petitioner,

v.

SUPERIOR COURT OF LOS ANGELES COUNTY,

Respondent;

ESCAPE MEDIA GROUP, LLC,

Real Party in Interest.

Petition for extraordinary writ. Richard Stone, Judge. Petition is granted.

McKenna Long & Aldridge, Charles A. Bird; Public Citizen Litigation Group,
Paul Alan Levy; Micah Gabriel Katz for Petitioner.

No appearance for Respondent.

McPherson Rane, Edwin F. McPherson and Pierre B. Pine; Rosenberg & Giger,
John J. Rosenberg for Real Party in Interest.
Escape Media Group (Escape) operates an Internet service called Grooveshark through which users may upload and retrieve digital music files. UMG Recordings, Inc. owns an extensive music catalog that includes songs by such artists as Buddy Holly, The Jackson 5, Marvin Gaye, and The Who. In 2010, UMG sued Escape in the Supreme Court of the State of New York, alleging Escape infringed on copyrights afforded by New York common law by reproducing user-uploaded, copyrighted sound recordings, storing them on its servers, and distributing copies to other users, to its own profit. Escape denied liability, asserting its conduct was permissible under federal copyright law.

Digital Music News (Digital) publishes the online newsletter Digital Music News, which focuses on the digital music industry. In 2011, Digital Music News reported that a music artist unaffiliated with UMG had also accused Escape of copyright infringement.

The article was followed by approximately 100 reader comments, two of which are of interest here. In them, a reader identified only as “Visitor” represented he or she was an Escape employee and routinely received “direct orders from the top” to upload music to its servers, where it was stored and made available to third party users and never removed, even if artists or music labels complained.

Under the auspices of the Supreme Court of the State of New York, County of New York, Escape served a subpoena on Digital (which is not a party to the litigation between UMG and Escape), seeking Visitor’s identity. When Digital refused to comply, Escape petitioned the Los Angeles Superior Court pursuant to the Interstate and International Depositions and Discovery Act, Code of Civil Procedure section 2029, et seq., for enforcement. The court ordered Digital to comply with the subpoena, from which order Digital now appeals.

Digital argues information identifying Visitor will not reasonably lead to the discovery of admissible evidence in the New York lawsuit and is protected by Visitor’s right to privacy. We agree with both contentions, and will therefore issue a writ of mandate directing the trial court to vacate its order enforcing Escape’s subpoena.
Statement of Facts

1. The New York Lawsuit

Grooveshark enables third party users to upload, share, download and stream files containing audio recordings. On January 6, 2010, UMG sued Escape in New York state court for state common law copyright infringement and unfair competition, alleging Escape enabled and encouraged Grooveshark users to upload unauthorized copies of UMG’s recordings to Grooveshark, which Escape then copied to its servers and subsequently distributed to other Grooveshark users. (UMG Recordings v. Escape Media Group (Supreme Ct. New York County, 2010, No. 100152).)\(^1\)

Escape denied the allegations and asserted a number of affirmative defenses and counterclaims. Among other defenses, Escape claimed immunity under the Digital Millennium Copyright Act (DMCA), which shields from federal copyright infringement liability an Internet service provider that hosts solely third party user materials, so long as it promptly removes copyrighted materials when it becomes aware of the infringement.\(^2\) (17 U.S.C. § 512(a)-(c).) On April 23, 2013, this defense was ordered stricken by the Appellate Division of the Supreme Court of New York on the ground that DMCA affords immunity only against federal copyright claims, not state common law claims. (UMG Recs., Inc. v. Escape Media Group, Inc. (N.Y. App.Div. 1st Dep’t 2013) 107 A.D.3d 51, 59.) In its answer, Escape also asserted counterclaims for interference with Escape’s

---

\(^1\) In its state lawsuit, UMG sought redress only as to recordings created prior to February 15, 1972. This is because the Copyright Act of 1976, title 17 United States Code section 101, et seq., expressly preempts state law copyright protections on material recorded on or after February 15, 1972. (17 U.S.C. § 301(a) & (c).)

\(^2\) Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act, 17 U.S.C. § 512, et seq., creates a safe harbor for an online service provider against copyright infringement liability if the provider meets specified requirements, one of which is the provider must promptly block access to alleged infringing material or remove the material from its systems when it receives notification of an infringement claim from a copyright holder.
contracts, interference with its business relations, and anti-competitive conduct, alleging UMG caused other companies to end their business relationships with Escape.³

In October 2011, Digital Music News reported on an email exchange between Escape executives and a member of a rock band who had complained that Grooveshark illegally hosted the band’s copyrighted recordings and refused to take them down. In the comments section of this article, Visitor claimed to “work for Grooveshark” and stated “the administration” required employees to upload files to the Grooveshark database, which contradicted Escape’s claim that it hosted solely third party recordings as permitted by the DMCA. The next day, Visitor⁴ commented that although Grooveshark administrators purported to remove copyrighted music when record labels and artists complained, the music was not actually deleted but merely put on “backup,” to be made available at a later time, when the complaining party’s attention turned elsewhere.

³ We deny Digital’s request for judicial notice of copyright infringement lawsuits brought against Escape by other music companies, as these cases are irrelevant to the issues before us. (See Arce v. Kaiser Found. Health Plan, Inc. (2010) 181 Cal.App.4th 471, 482 [“We also may decline to take judicial notice of matters that are not relevant to dispositive issues on appeal”].)

⁴ It is possible the anonymous comments were written by two different authors. Because the parties assume one author wrote both comments, we will also.
Visitor stated the music was in fact never deleted: “[T]o confirm the fears of [complaining musicians], there is no way in hell you can get your stuff down.”

2. The Subpoena and Enforcement

On January 9, 2012, Escape served Digital with a subpoena in the New York action for the production of business records, seeking information concerning Visitor’s identity and communications between Digital and UMG concerning, or documents relating to, Escape, Grooveshark, or the October 2011 Digital Music News article. Digital objected to the subpoena and notified Escape that any information about Visitor’s

---

5 On October 17, 2011, Visitor said: “I work for [Escape]. Here is some information from the trenches: [¶] We are assigned a predetermined amount of weekly uploads to the system and get a small extra bonus if we manage to go above that (not easy). The assignments are assumed as direct orders from the top to the bottom, we don’t just volunteer to ‘enhance’ the . . . database. [¶] All search results [user searches of the database] are monitored and when something is tagged as ‘not available’, it get’s [sic] queued up to our lists for upload. You have to visualize the database in two general sections: ‘known’ stuff and ‘undiscovered/indie/underground’. The ‘known’ stuff is taken care internally by uploads. Only for the ‘undiscovered’ stuff are the users involved as explained in some posts above. Practically speaking, there is not much need for users to upload a major label album since we already take care of this on a daily basis. [¶] Are the above legal, or ethical? Of course not. Don’t reply to give me a lecture. I know. But if the labels and their laywers [sic] can’t figure out how to stop it, then I don’t feel bad for having a job. It’s tough times. [¶] Why am I disclosing all this? Well, I have been here a while and I don’t like the attitude that the administration has acquired [sic] against the artists. They are the enemy. They are the threat. The things that are said internally about them would make you very very angry. Interns are promised getting a foot in the music industry, only to hear these people cursing and bad mouthing the whole industry all day long, to the point where you wonder what would happen if [the Web site] gets hacked by Anonymous one day and all the emails leak on some torrent or something. [¶] And, to confirm the fears of the members of [the complaining music artist], there is no way in hell you can get your stuff down. They are already tagged since you sent in your first complaint. The administration knows that you can’t afford to sue for infringement.”

On October 18, 2011, Visitor said: “Just because you can’t see an album available right now, doesn’t mean it’s not sitting quietly in the background. It is policy to put albums on ‘backup’, when they have to be taken down due to a [copyright claim], to chill things out with the labels and what not. The albums are not deleted, if that’s what you guys think.”
identity had been deleted as part of Digital’s routine business practice of periodically overwriting data.

On March 20, 2012, Escape petitioned the Los Angeles County Superior Court to enforce the subpoena under the Interstate and International Depositions and Discovery Act, Code of Civil Procedure section 2029 et seq. Digital opposed the petition, arguing the subpoena was moot because any information that would identify Visitor had been overwritten, enforcement of the subpoena would infringe on the First Amendment rights of Digital and Visitor, and disclosure would violate California’s journalist shield law (Cal. Const., art. I, § 2, subd. (b); Evid. Code, § 1070). In reply, Escape argued Digital had no basis for refusing to comply with the subpoena because the First Amendment does not protect false and defamatory anonymous speech.

Although Digital denied any discoverable material remained on its servers, the trial court found a possibility existed that fragmented data identifying Visitor might yet be retrieved. The court also found Escape established a prima facie case that Visitor’s comments were libelous, and thus unprotected by the First Amendment. The court concluded Visitor’s identity was therefore discoverable and ordered Digital to comply with the subpoena.

The trial court subsequently issued a supplemental order addressing the compliance process. The court ordered Escape to purchase and provide Digital with a

All further statutory references are to the Code of Civil Procedure unless otherwise indicated.

On appeal, Digital has abandoned its argument under California’s journalist shield law.

The court ordered Digital to produce: “[A]ny and all business records (including, without limitation, e-mail files, databases, logs of activity on computer systems and/or content and information contained within the [Digital] website or administrative panel, or any backup copies of the data from within either) that [Digital] has concerning the” first and second anonymous comments, or its author, the person identified by the pseudonym Visitor. The court’s order did not address the portion of the subpoena seeking communications and/or documents concerning Escape, Grooveshark, or the October 2011 Digital Music News article. Escape has not pursued that discovery.
backup server, and ordered Digital to preserve a virtual machine image of its server on the backup server and make the image available to a third party forensic examiner under court supervision. The examiner would first indicate to Digital whether any identifying information was present and then reveal such information to Escape if directed to do so by the court. Escape would pay all expenses related to the data preservation and inspection. Once the inspection was complete, the backup server would be expunged of any material.9

Digital timely appealed both orders and we issued a writ of supersedeas staying discovery. Pursuant to our request, the parties submitted supplemental letter briefs addressing whether section 2017.010 and the California Constitution’s right of privacy preclude discovery of Visitor’s identity.

Discussion

1. Standard of Review

Pursuant to the Interstate and International Depositions and Discovery Act, a party to a proceeding in a foreign jurisdiction may obtain discovery in California by retaining a local attorney to issue a subpoena. (§ 2029.350.) If a dispute arises relating to the subpoena, any party may petition the superior court where the discovery is to be conducted for a protective order or an order enforcing, quashing, or modifying the subpoena. (§ 2029.600.) Such an order may be reviewed only by petition to the Court of Appeal for an extraordinary writ. (§ 2029.650, subd. (a).) Although Digital filed an appeal here, we deem the appeal to be a writ petition.

A discovery order is reviewed under the deferential abuse-of-discretion standard. (Krinsky v. Doe 6 (2008) 159 Cal.App.4th 1154, 1161.) An appellate court may reverse a trial court decision for abuse of discretion when the trial court “applies the wrong legal standards applicable to the issue at hand.” (Doe 2 v. Superior Court (2005) 132 Cal.App.4th 1504, 1517.)

---

9 Currently, Digital has transferred a virtual machine image of its server to the backup server provided by Escape, but no other action has been taken.
2. **California discovery law prohibits disclosure of Visitor’s identity**

Although discovery sought under the Interstate and International Depositions and Discovery Act is intended for use in a foreign jurisdiction, it is nevertheless governed by California’s Civil Discovery Act, section 2016.010 et seq. (§ 2029.500.) Section 2017.010 of that act sets forth the permissible scope of discovery in California: “[A]ny party may obtain discovery regarding any matter, not privileged, that is relevant to the subject matter involved in the pending action . . . if the matter either is itself admissible in evidence or appears reasonably calculated to lead to the discovery of admissible evidence.” (§ 2017.010.) A party may also obtain discovery of “the identity and location of persons having knowledge of any discoverable matter, as well as of the existence, description, nature, custody, condition, and location of any document [or] electronically stored information . . . .” (Ibid.)

An appellate court may reverse a trial court’s grant of discovery if it concludes the information sought “cannot as a reasonable possibility lead to the discovery of admissible evidence or be helpful in preparation for trial.” (Forthmann v. Boyer (2002) 97 Cal.App.4th 977, 988-989.) Only relevant evidence is admissible. (Evid. Code, § 350.) Relevant evidence is that which has a “tendency in reason to prove or disprove any disputed fact that is of consequence to the determination of the action.” (Evid. Code, § 210.)

“Although the scope of civil discovery is broad, it is not limitless.” (Calcor Space Facility, Inc. v. Superior Court (1997) 53 Cal.App.4th 216, 223.) Discovery devices must “be used as tools to facilitate litigation rather than as weapons to wage litigation.” (Id. at p. 221.) A party seeking to compel discovery must therefore “set forth specific facts showing good cause justifying the discovery sought.” (§ 2031.310, subd. (b)(1); see Calcor Space Facility, Inc. v. Superior Court, supra, 53 Cal.App.4th at p. 223.) To establish good cause, a discovery proponent must identify a disputed fact that is of consequence in the action and explain how the discovery sought will tend in reason to prove or disprove that fact or lead to other evidence that will tend to prove or disprove the fact.
The facts of consequence in the New York lawsuit between UMG and Escape may be found in UMG’s complaint and Escape’s affirmative defenses and counterclaims.

In the New York lawsuit, UMG alleges Escape infringed on its common law copyrights and engaged in unfair competition. “A copyright infringement cause of action in New York consists of two elements: (1) the existence of a valid copyright; and (2) unauthorized reproduction of the work protected by the copyright.” (Capitol Records, Inc. v. Naxos of Am., Inc. (2005) 4 N.Y.3d 540, 563.) A cause of action for unfair competition predicated on copyright infringement, “in addition to unauthorized copying and distribution requires competition in the marketplace or similar actions designed for commercial benefit [citations], or deception of the public [citation].” (Id. at pp. 563-564.) UMG alleges Escape “enables and encourages its users to upload digital copies” of UMG’s recordings to Grooveshark, then copies those recordings to its servers and distributes them to other users. By doing so, Escape infringes on UMG’s copyrights and unfairly competes with UMG for commercial benefit.

In its answer, Escape denies the allegations and contends its conduct is permitted under the DMCA. Title II of that act provides in pertinent part: “A service provider shall not be liable . . . for infringement of copyright by reason of” transmission or storage of transitory digital information so long as the transmission or storage is done “at the direction of a person other than the service provider,” is “carried out through an automatic technical process without selection of the material by the service provider,” and does not result in copies of the material being maintained on the system or network “for a longer period than is reasonably necessary for the transmission.” (17 U.S.C. § 512(a) & (b).) To enjoy this immunity, a service provider who becomes aware of infringing material on its network must “respond[ ] expeditiously to remove, or disable access to, the material.” (17 U.S.C. § 512(c)(1)(C).) As stated above, Escape’s DMCA defense was ordered stricken by the appellate division of the New York Supreme Court.

Escape also counterclaims for interference with its contracts and business relations and anti-competitive conduct. Under New York law, “[t]o sustain a claim for tortious interference with a contract, it must be established that a valid contract existed which a
third party knew about, the third party intentionally and improperly procured the breach of the contract[,] and the breach resulted in damage to the plaintiff.” (Ullmann glass v. Oneida, Ltd. (2011) 927 N.Y.S.2d 702, 705.) Where there has been no breach of an existing contract, but only interference with prospective contract rights, the plaintiff must show the defendant’s conduct amounted to a crime or an independent tort. (Carvel Corp. v. Noonan (2004) 3 N.Y.3d 182, 190.) Escape alleges UMG has engaged in a “legal jihad” in which it coerces third party companies to breach their contracts with Escape and terminate beneficial relationships, the goal being “to destroy Escape by cutting off [its] sources of revenue.”

It was not readily apparent to us how the identity of Visitor, who, similar to UMG, claimed Escape routinely violated copyrights on sound recordings, would lead to admissible evidence refuting UMG’s allegations or supporting Escape’s defenses or counterclaims. We therefore asked Escape to explain in a supplemental brief how discovery of Visitor’s identity was reasonably calculated to lead to the discovery of admissible evidence.

Escape first states without elaboration that Visitor’s identity is “most assuredly” relevant to Escape’s DMCA defense. This is a conclusion, not an explanation, much less a showing of specific facts demonstrating discovery of Visitor’s identity is reasonably calculated to lead to admissible evidence. To establish its DMCA defense Escape would have had to prove, among other things, that it removes copyrighted material when informed of an infringement. Escape fails to explain how the identity of Visitor—who claims the opposite—would lead to evidence supporting the defense.

In any event, Escape’s DMCA defense was ordered stricken by the Appellate Division of the New York State Supreme Court, which held the defense immunizes a service provider only from federal copyright claims, not state common law claims such as those at issue here. The defense therefore raises no currently disputed “fact that is of consequence to the determination of the action” (Evid. Code, § 210), rendering Visitor’s comments irrelevant.
Escape insists that the viability of its DMCA defense “is far from resolved with either finality or certainty,” because in *Capitol Records v. Vimeo* (S.D.N.Y. Dec. 31, 2013) 2013 U.S.Dist. Lexis 181882 (*Vimeo*), the United States District Court for the Southern District of New York certified an interlocutory appeal on the DMCA immunity issue to the United States Court of Appeals for the Second Circuit. But this merely establishes the possibility that Escape’s DMCA defense might someday be reinstated—assuming the Second Circuit accepts the *Vimeo* appeal, and rules DMCA immunity applies to state common law claims, and Escape moves on that basis to reinstate its DMCA defense, and the New York Supreme Court grants the motion. Speculation about a remote-in-time possibility does not constitute reasonable calculation that discovery will lead to evidence concerning a fact currently in dispute.

Escape next argues Visitor’s comments are relevant to any claim by UMG that Escape may be secondarily liable for infringement of UMG’s copyrights. Escape argues it must identify Visitor “as a predicate to exposing the Anonymous Comments as false,” which will refute any allegation that Escape knew about or supervised direct infringement of UMG’s copyrights by Escape employees.

The argument is meritless. First, UMG makes no allegation pertaining to secondary liability based on the conduct of Escape’s employees. Rather, it alleges Escape enables Grooveshark users to upload music, which is then copied, stored, and distributed to other users. “Relevant evidence” means evidence “having any tendency in reason to prove or disprove any disputed fact that is of consequence to the determination of the action.” (Evid. Code, § 210, italics added.) Escape’s operation of Grooveshark in the manner UMG alleges is not in dispute, as Escape expressly admitted the practice in its answer. The only issue is whether the practice violates UMG’s copyrights, which is a
question of law, not fact. Although Escape contends Visitor’s comments are untrue, that out-of-court quarrel is of no consequence to the determination of UMG’s lawsuit.  

Even if UMG had alleged—perhaps in response to Escape’s now-defunct DMCA defense—that Escape employees personally uploaded copyrighted music to Grooveshark’s database and refused to take it down when asked, Escape still fails to explain how discovery of Visitor’s identity would tend in reason to lead to evidence disproving UMG’s allegation. Visitor said two things of consequence: (1) He/she is an Escape employee; and (2) Escape administrators encouraged employees to infringe on copyrights. Escape apparently believes disproving one or both of these out-of-court claims would somehow disprove UMG’s allegations. We fail to see how. Even if Escape were able to show Visitor lacked evidence to support his or her claims—for example by showing Visitor was not in fact an Escape employee or was motivated by mischief or spite—such a showing would have no tendency in reason to prove UMG lacked evidence supporting its allegations. If Escape proposes to demonstrate affirmatively that its practices are not as Visitor described, Visitor’s identity would be unnecessary to such a proof. In either case, Visitor’s identity has no tendency in reason to prove or disprove any disputed fact of consequence to the action, and is not reasonably calculated to lead to such proof.

Escape argues Visitor’s identity “would obviously be germane” to its counterclaims for interference with business relations if, as Escape has long suspected, Visitor’s comments were planted by UMG. The argument is without merit.

In its counterclaims, Escape alleges that in 2010, UMG contacted Hewlett Packard, INgrooves (a digital music distribution company), Apple iStore, Google, and MusicAds (a Madrid, Spain company that sells ad space on Web sites) and dissuaded them from doing business with Escape. Nothing in the record suggests Escape’s

---

10 Nothing in the record suggests UMG will rely on Visitor’s assertion that Escape employees uploaded music to Grooveshark’s database, to support either of its causes of action. In fact, in response to Escape’s discovery request, UMG indicated it possessed no information related to Visitor’s identity.
counterclaims pertain in any way to Visitor’s 2011 comments on the Digital Music News Web site or that those comments caused third party companies to end business relationships or terminate contracts with Escape. Moreover, Escape offers no explanation supporting its belief that Visitor might be associated with UMG. Escape’s argument that Visitor is a UMG plant rests on pure speculation, not reasonable calculation.

Finally, Escape argues Visitor’s identity is relevant to a federal lawsuit in which UMG specifically references Visitor’s comments to bolster its allegation that Escape engaged in copyright infringement. In 2011, UMG and several other record labels filed a lawsuit in the Southern District of New York against Escape for violation of federal copyright laws.\(^\text{11}\) (Arista Music v. Escape Media Group (S.D.N.Y. 2011, No. 8407).) For reasons discussed above, we suspect Visitor’s identity would be irrelevant even in that lawsuit, as an anonymous comment on the Internet is nugatory both as a matter of pleading and of proof, and would not rise to the status of a disputed fact until such time as the plaintiff attempts to call Visitor into court. At any rate, allegations in another lawsuit are of no consequence to the determination of this action.

In sum, Visitor’s identity is not reasonably calculated to lead to the discovery of admissible evidence in the underlying lawsuit between UMG and Escape.

3. **Visitor’s privacy interests outweigh Escape’s need for disclosure**

Even if Visitor’s identifying information was reasonably calculated to lead to admissible evidence, his or her right to privacy under the California Constitution would outweigh Escape’s need for the information.\(^\text{12}\) “The right to speak anonymously draws its strength from two separate constitutional wellsprings: the First Amendment’s freedom

---

\(^\text{11}\) We deny Digital’s request for judicial notice of memoranda of law relating to Escape’s motion to dismiss in this federal case. As the subpoena in the case before us arises out of UMG’s lawsuit against Escape in New York state court, these memoranda are irrelevant.

\(^\text{12}\) Digital possesses standing to assert Visitor’s constitutional rights. (See Rancho Publications v. Superior Court (1999) 68 Cal.App.4th 1538, 1541 [a non-party “to civil litigation (such as a newspaper) [may] assert the constitutionally protected rights of an author to remain unknown”].)
of speech and the right of privacy in article I, section 1 of the California Constitution.” (*Rancho Publications v. Superior Court, supra*, 68 Cal.App.4th at pp. 1540-1541.) The California Constitution provides that all people have a right of privacy. (Cal. Const., art. I, § 1.) This express right is broader than the implied federal right to privacy. (*American Academy of Pediatrics v. Lungren* (1997) 16 Cal.4th 307, 326.) The California privacy right “protects the speech and privacy rights of individuals who wish to promulgate their information and ideas in a public forum while keeping their identities secret,” and “limits what courts can compel through civil discovery.” (*Rancho Publications v. Superior Court, supra*, 68 Cal.App.4th at pp. 1547-1548.)

Both California courts and federal courts have recognized the value in extending the protections afforded anonymous speech to speech made via the Internet. (See generally *Reno v. ACLU* (1997) 521 U.S. 844, 870; *Krinsky v. Doe 6, supra*, 159 Cal.App.4th 1154.) “The use of a pseudonymous screen name offers a safe outlet for the user to experiment with novel ideas, express unorthodox political views, or criticize corporate or individual behavior without fear of intimidation or reprisal. In addition, by concealing speakers’ identities, the online forum allows individuals of any economic, political, or social status to be heard without suppression or other intervention by the media or more powerful figures in the field.” (*Krinsky v. Doe 6, supra*, 159 Cal.App.4th at p. 1162.) “The ‘ability to speak one’s mind’ on the Internet ‘without the burden of the other party knowing all the facts about one’s identity can foster open communication and robust debate.’” (*Doe v. 2TheMart.com Inc.* (2001) 140 F.Supp.2d 1088, 1092.)

“[W]hen the constitutional right of privacy is involved, the party seeking discovery of private matter must do more than satisfy the section 2017[.010] standard. The party seeking discovery must demonstrate a compelling need for discovery, and that compelling need must be so strong as to outweigh the privacy right when these two competing interests are carefully balanced.” (*Lantz v. Superior Court* (1994) 28 Cal.App.4th 1839, 1853-1854; see also *Planned Parenthood Golden Gate v. Superior Court* (2000) 83 Cal.App.4th 347, 367 [courts must balance the privacy interests of the person subject to discovery against the litigant’s need for discovery].) A discovery
proponent may demonstrate compelling need by establishing the discovery sought is directly relevant and essential to the fair resolution of the underlying lawsuit. (Planned Parenthood Golden Gate v. Superior Court, supra, 83 Cal.App.4th at p. 367; Johnson v. Superior Court (2000) 80 Cal.App.4th 1050, 1071.)

Applying this balancing test we conclude Visitor’s privacy interest outweighs Escape’s need to discover his or her identity. That interest begins with Visitor’s need for a venue from which to be heard without fear of interference or suppression. Visitor’s anonymity also frees him or her from fear of retaliation, an even more compelling interest if Visitor truly is an Escape employee, as represented, because exposure could endanger not only his or her privacy but also livelihood.

On the other hand, Escape’s need for the discovery is practically nonexistent. If Visitor is not an Escape employee, his or her opinion about Grooveshark not only lacks foundation but would be undermined by Visitor’s misrepresentation concerning employment, and would therefore be of little or no probative value in this or any litigation. And as discussed above, Visitor’s comments, even if made by an employee, are only tangentially related to UMG’s lawsuit, as Visitor makes allegations UMG does not make and undermines a defense Escape is now barred from raising.

In no sense is Visitor’s identity essential to a fair resolution of the UMG lawsuit. This is not a case where the veil of anonymity must be drawn aside to afford a victim redress for the anonymous speaker’s defamation (Krinsky v. Doe 6, supra, 159 Cal.App.4th at pp. 1666-1667, 1173), obscenity (Roth v. United States (1957) 354 U.S. 476, 483), libel (Beauharnais v. Illinois (1952) 343 U.S. 250, 266), copyright infringement (Harper & Row, Publishers, Inc. v. Nation Enterprises (1985) 471 U.S. 539, 555-556), misleading or commercial speech (Central Hudson Gas & Electric Corp. v. Public Service Comm’n (1980) 447 U.S. 557, 563-564), or use of ‘fighting words’ (Chaplinsky v. New Hampshire (1942) 315 U.S. 568, 573). Visitor has done nothing more than provide commentary about an ongoing public dispute in a forum that could hardly be more obscure—the busy online comments section of a digital trade newspaper. Such commentary has become ubiquitous on the Internet and is widely perceived to carry
no indicium of reliability and little weight. We will not lightly lend the subpoena power of the courts to prove, in essence, that Someone Is Wrong On The Internet.

Given our holdings above, we decline to address Digital’s argument that routinely deleted data controlled by a non-party cannot be subject to forensic examination under the principles of electronic discovery.

Dispersion

The petition for writ of mandate is granted. The trial court is directed to vacate its order granting Escape’s petition to enforce the subpoena and to enter a new order denying the petition. The writ of supersedeas is dissolved. Digital is to recover its costs on appeal.

CERTIFIED FOR PUBLICATION

CHANNEY, J.

We concur:

ROTHSCHILD, Acting P. J.

JOHNSON, J.