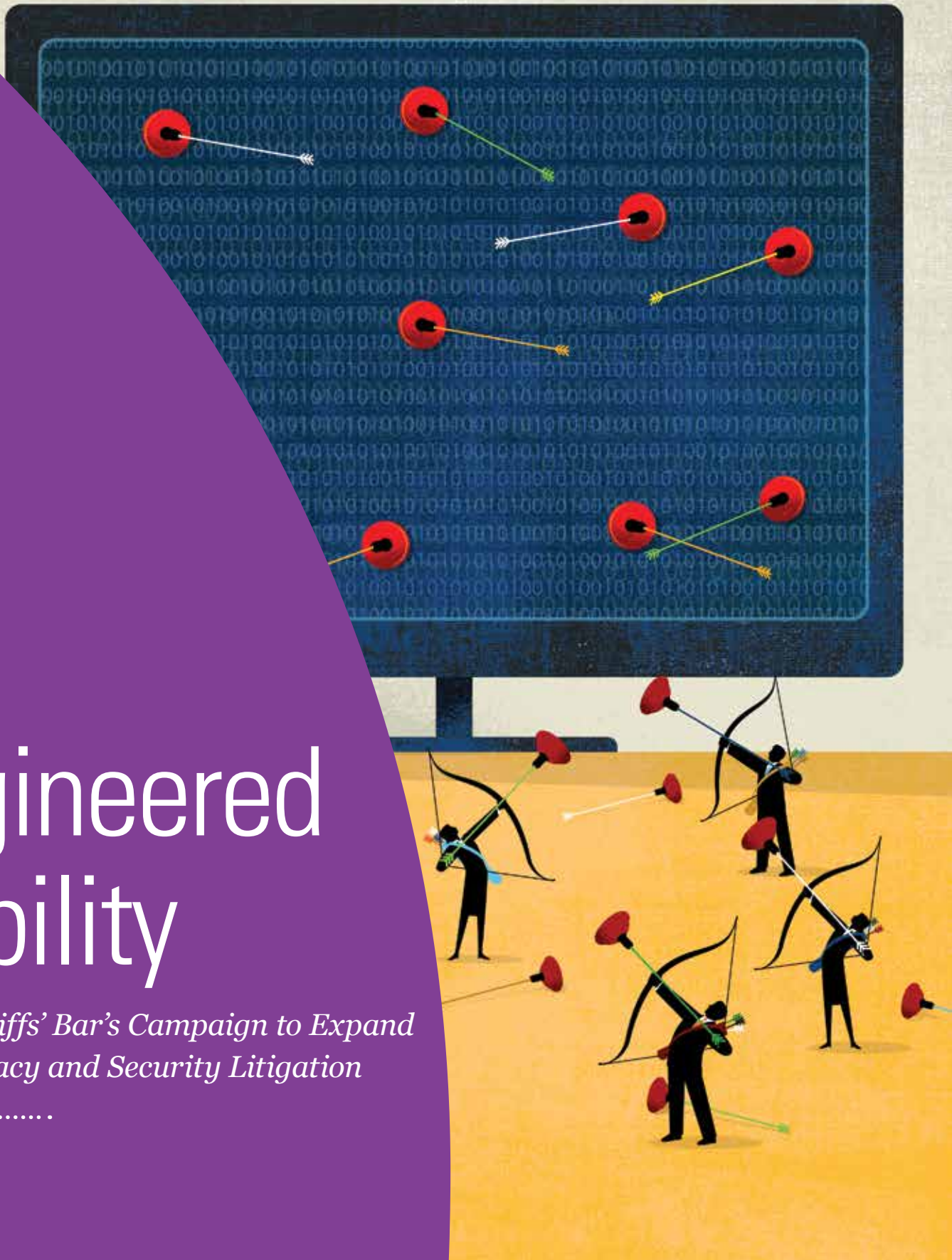
U.S. CHAMBER
Institute for Legal Reform



Engineered Liability

The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation

APRIL 2017

U.S. CHAMBER
Institute for Legal Reform

An Affiliate of the U.S. Chamber of Commerce

Table of Contents

Prepared for the U.S. Chamber Institute for Legal Reform by

Divonne Smoyer and Kimberly Chow, Reed Smith LLP

Executive Summary

When the prospect of large monetary settlements is on the table, no business sector is secure from plaintiffs' attorneys. In this pattern, there is a growing campaign by the plaintiffs' bar to target data privacy and security in the hopes of striking it rich in a new goldmine on the level of the asbestos litigation of the 1970s, 80s, and 90s. The plaintiffs' bar appears to be taking advantage of the unfortunate reality that data breaches are becoming more commonplace, privacy laws and regulations in the U.S. are in flux, federal and state regulators are hungry for a new privacy framework, and consumers and citizens are confused about what protections, if any, apply to their information. In doing so, plaintiffs' attorneys are undertaking to expand regulation of and legal exposures for businesses in this area and also are stretching old laws to address new situations involving privacy in unintended ways.

Plaintiffs' attorneys are engineering a staggering expansion of liability in the areas of privacy and data security. Class action lawyers are pursuing data privacy cases and amassing fortunes even where no one has been harmed. An alleged "breach" may have resulted when a laptop was lost, for example, but if the information on it was never accessed, no identity theft or other damage will have resulted. But the absence of actual harm does not stop plaintiffs from pursuing legal theories such as "unjust enrichment," among others.

> *"Class action lawyers are pursuing data privacy cases and amassing fortunes even where no one has been harmed."*

In privacy and security breaches, as in many other types of claims, the plaintiffs' bar does not draw distinctions between culpable and non-culpable conduct. A class action lawsuit is bound to follow regardless of whether an entity that suffered a security breach was the target of state-sponsored cyberterrorism or whether it was in fact negligent. The theories in seeking monetary recovery range from violations of the breach notification laws themselves to state deceptive trade practices laws, which are notoriously vague and often exploited. Plaintiffs' attorneys press hard to expand theories of liability, often putting new twists on old torts such as conversion (the appropriation of another's goods). In addition, they often seek out cases they believe will yield a big payday, and only then try to find a class representative to name in their complaint. Indeed, one tactic for identifying cases is to comb state attorney general websites for breach notifications.

Between the new liability theories and the aggressive tactics for creating cases, the number of data privacy class actions has exploded over the past few years. Between the third quarter of 2013 and the third quarter of 2014, plaintiffs filed approximately 672 data privacy complaints in U.S. district courts, with nearly one-third of all data privacy litigation filed in California federal courts.[1] The BTI Business Development Opportunity Zones report for 2016 predicted that the market size in outside counsel spending in light of these suits would grow from $1.5 billion in 2015 to $1.67 billion in 2016.[2] And according to the 2016 Cost of Data Breach Study by IBM and the Ponemon Institute LLC, U.S. companies spent an average of $7.01 million each on data breaches in 2015, a figure which includes legal expenditures before and after a breach.[3]

"U.S. companies spent an average of $7.01 million each on data breaches in 2015, a figure which includes legal expenditures before and after a breach."

Consumers are not primarily driving these changes—certain plaintiffs' firms are responsible for a large portion of the litigation explosion. Four plaintiffs' firms, or 1.5 percent of the 240 firms that filed data privacy complaints in the period between the third quarter of 2013 and the third quarter of 2014, accounted for over a third of the complaints filed.[4] As one may expect, the American Association for Justice (AAJ), the national organization of plaintiffs' attorneys, also has privacy in its crosshairs. It has formed a specific consumer privacy/data litigation group, which works to compile knowledge and documents from similar cases, identify successful litigation strategies, and bring together a network of attorneys to provide each other with advice.[5]

These cases seldom provide much, if anything, by way of compensation to the actual claimants in the class actions. One notorious example is the suit against Facebook's Beacon Ad program, which displayed Facebook users' purchases and video rentals.[6] From that settlement the plaintiffs' lawyers received $2.3 million. Class members received nothing, and Facebook paid $6.5 million to a new foundation it would partly control that would research privacy rights.[7]

This paper addresses how the plaintiffs' bar is adapting to and taking advantage of the ever-changing data privacy and security legal landscape. It explores major privacy cases and settlements, showing how the plaintiffs' bar is targeting breaches and other privacy violations. It also profiles the major firms that bring a large proportion of the cases—including Edelson PC and Lieff Cabraser Heimann & Bernstein LLC—along with the tactics they employ to create privacy cases and take aim at defendants, and the theories that they have been testing in the courts. Finally, the paper offers a framework for reform.

Privacy Cases and the Firms That Bring Them

Similar to the asbestos litigation of the last century, plaintiffs' lawyers have detected a potential goldmine in targeting liability in connection with data privacy and security, and have rushed to reap the benefits. A large number of high-profile, multi-million dollar settlements and the increasing visibility of the firms that bring many of these cases show that this is a growing, profitable business with major players.

Major Data Privacy and Breach Cases

A litany of well-publicized class actions and settlements illustrate how the plaintiffs' bar is pushing the boundaries of data privacy liability.

Whenever a data breach becomes public, whether a hostile foreign government engineered the attack or the company was in fact negligent, lawsuits and negative publicity are quick to follow. For instance, after hackers accessed the credit card information of Target customers, the company paid $10 million to settle a federal consumer class action lawsuit.[8] Consumers argued that the breach could have been avoided had Target properly protected its systems, and they alleged harms ranging from identity theft to reimbursement for purchases made during the breach, which they said they would not have made had they been notified of the breach.[9] The attorneys in the consumer class action would eventually receive up to $6.75 million in fees.[10]

Sony, the victim of hacks likely backed by the government of North Korea, agreed to pay as much as $8 million to settle employee claims regarding the exposure of their personal information in a computer hack.[11] The employees were awarded $4.5 million as a class, while the plaintiffs' lawyers were awarded almost as much—$3.5 million.[12]

Meanwhile, fifty-seven proposed class actions against Home Depot were consolidated in an Atlanta U.S. District Court, resulting in a settlement of $19.5 million to compensate customers whose credit card information had been exposed, with at least $8.7 million going to the attorneys.[13] In March 2017, retailer Neiman Marcus, which had been targeted by Russians for customer credit card information, agreed to settle for $1.6 million.[14] The class action against health insurance company Anthem Inc., which was purportedly attacked by Chinese hackers,[15] is moving through the court system.[16]

Even the government is not immune. Following the hacking of 330,000 taxpayers' information in the Internal Revenue Service's online Get Transcript application, the Internal Revenue Service (IRS) was hit with class actions as well.[17] Ironically, in its arguments against IRS liability, the Department of Justice argued that the plaintiffs did not have standing to sue because they had not been harmed.[18] Yet the federal government made exactly the opposite argument—that a technical breach of privacy without further harm was enough to confer standing—before the U.S. Supreme Court in the *Spokeo* case.

It is not only high-profile breaches that attract litigation. Some of the most publicized data privacy class actions have involved not breaches, but attempts to capitalize on technical violations of privacy laws. *Spokeo, Inc. v. Robins*, which the U.S. Supreme Court decided in May 2016, involved a plaintiff's claim that a data broker had violated his privacy under the federal Fair Credit Reporting Act by publishing incorrect information about him online.[19]

> *"Some of the most publicized data privacy class actions have involved not breaches, but attempts to capitalize on technical violations of privacy laws."*

Likewise, suits filed against streaming services such as Netflix have alleged violations of the federal Video Privacy Protection Act when a company retains customers' streaming information after they closed their accounts.[20] Netflix settled for $9 million, with $2.25 million going to the plaintiffs' lawyers.

The Telephone Consumer Protection Act and Other Abused Laws

Arguably, the most widely abused law relating to data privacy is the Telephone Consumer Protection Act (TCPA). Sixty-five percent of all data privacy-related class actions from the third quarter of 2013 to the third quarter of 2014 involved the TCPA, a 1991 law that has proved to be a boondoggle for plaintiffs' lawyers through its grant of automatic statutory damages for calls and texts sent without prior permission.[21]

The original intent of the law—to protect consumers from unwanted telemarketing calls—has been eclipsed by the avalanche of abusive litigation that has resulted. Subsequent clarifications of the law to address cell phones and forms of consent have increased the compliance burden on companies, who now must obtain "prior express written consent" for autodialed or prerecorded marketing calls, even when placed to their own customers. The law automatically assesses a $500 penalty for each call or text violating the TCPA, but those damages can be trebled to $1,500 if the court decides that the defendant "willfully or knowingly" violated the statute.

> *Sixty-five percent of all data privacy related class actions from the third quarter of 2013 to the third quarter of 2014 involved the TCPA…*

The litigation activity that has proliferated around the law is staggering. One law firm, Lemberg Law, has even developed a free app, "Block Calls Get Cash," that consumers can use to track potentially illegal calls from telemarketers and deliver information about the calls to the firm so that it can bring suits. Promising that users can "collect up to $1,500 per call," the app claims to have recovered $30 million for 10,000 people.[22]

State laws are also often-used tools for driving litigation. One example of a state law targeting new technology that has become a vehicle for privacy complaints is the Illinois Biometric Information Privacy Act, which prescribes specific notice, consent, and data retention requirements for entities that collect biometric data, such as fingerprints or retina scans.[23] The law firm Edelson PC is leading a class action in Illinois against Facebook, alleging that the company violated the Illinois law by collecting the facial geometry of users and non-users who appear in photos uploaded to the social networking site, for the purpose of suggesting that they be "tagged."[24] Shutterfly settled a similar class action brought pursuant to the same law in April 2015 for an undisclosed amount.[25]

Alaska's Genetic Privacy Act is another example of a state law attracting a new crop of class actions. The Act limits access, retention, and sharing of genetic data.[26] In 2014, Edelson PC sued the company Family Tree DNA for publishing the results of customers' ancestry research on its public website.[27] The plaintiffs sought statutory damages of $5,000, or, if the plaintiffs could prove that the violation resulted in profit or monetary gain to Family Tree DNA, $100,000 for each litigant.[28]

Major Firms Driving Litigation

Certain plaintiffs' firms are class action factories, with their sights trained on taking advantage of perceived deep pockets in this expanding area of liability. The resulting frenzy surrounds not just the tech sector, but every industry that processes individuals' information.

Edelson PC has risen to prominence as one of the most aggressive firms in this area. The law firm, based in Chicago, has "gone after pretty much every tech company you have heard of—Amazon, Apple, Google—as well as many that you have not."[29] In fact, Edelson has made such a name for itself in capitalizing on new technologies that the firm and its founder, Jay Edelson, were the subject of a critical *New York Times* article: "Jay Edelson, the Class-Action Lawyer Who May Be Tech's Least Friended Man."[30]

> *"In the law firm breach case, Edelson is alleging that the Chicago firm's clients 'have been overpaying for legal services—because they have been paying, in part, to keep their data secure—and the law firm hasn't been keeping up with their end of the bargain.'"*

An example of how Edelson capitalizes on companies' misfortune surrounding data losses arose after the announcement in March 2016 of security breaches at several high-profile law firms. Edelson had conducted a year-long investigation to identify law firms with "inadequate cybersecurity,"[31] and had supposedly unearthed evidence upon which to base a lawsuit. Edelson filed a putative privacy class action against a Chicago firm for poor cybersecurity and stated that he plans to bring malpractice class actions against other firms over the exposure of client information.[32] The privacy suit was originally filed under seal, but after Edelson developed its case, it moved to make it public and provide an example of how to bring future cases. Jay Edelson tweeted at the time, "Moving to unseal #datasecurity #privacy #classaction complaint against Chicago law firm. If granted, all pleadings will be public. #roadmap."[33] The case has now moved to arbitration, and Edelson is seeking arbitration as a class.[34]

This is Edelson's roadmap to success: By floating new theories targeting novel harms, the plaintiffs' lawyer business model is enhanced. Besides taking advantage of the privacy vulnerabilities of new technologies, he has invented new ways to claim plaintiffs have been harmed. In the law firm breach case, Edelson is alleging that the Chicago firm's clients "have been overpaying for legal services—because they have been paying, in part, to keep their data secure—and the law firm hasn't been keeping up with their end of the bargain."[35]

Edelson has made its presence known in many recent big data privacy cases, bringing suit against companies from Spokeo to Netflix, and claims to have garnered over $1 billion in settlements.[36] Over the past five years, Edelson PC has filed more than 150 complaints involving consumer privacy.[37] A large portion of those complaints were TCPA-related. About 20 complaints related to data breach incidents, and the other complaints involved various claims alleging violations of state and federal privacy laws.

Other law firms have also been active in targeting data privacy and security. They have preyed on cyberattacks and new technologies and harms, including biometric data.

- Lieff Cabraser Heimann & Bernstein, LLP, based in San Francisco, has had a hand in privacy suits ranging from the well-publicized breaches at Anthem and Sony to cases involving the retention of children's information after they played with the "Hello Barbie" toy. The firm has also taken on the inaccuracy of credit reports issued by Equifax and TransUnion, Google's automated scanning of the content of Gmail messages, TurboTax's processing of fake tax returns, and many others. In total, Lieff Cabraser has filed approximately 75 complaints involving consumer privacy over the past five years, including many TCPA complaints.[38]

- Robbins Geller Rudman & Dowd LLP, based in San Diego, is involved in the Sony breach case and, like Edelson, has targeted biometric data as a new area to expand liability. The firm is representing the plaintiffs in a suit under the Illinois Biometric Information Privacy Act, alleging that Facebook's use of facial recognition technology to automatically tag pictures is a violation of the Act.[39]

- Scott Kamber of KamberLaw, LLC, based in New York, is a former partner of Jay Edelson. His firm has brought suits over allegedly unauthorized cookie placement and tracking of individuals' online activities, including by Walgreen Co. and Toys"R"Us.[40] He is perhaps best known for his suit against Facebook's Beacon Ad program, which displayed Facebook users' purchases and video rentals.[41] Under the settlement of that case, the lawyers received $2.3 million, class members received nothing, and Facebook paid $6.5 million to a new foundation it would partly control, that would research privacy rights.[42]

Plaintiffs' Firms Are Expanding with Privacy in Mind

Through strategic venue choices and new hires, plaintiffs' firms are investing in the privacy area, and it is paying off. The district courts of California are where many of the privacy battles are being fought, accounting for one third of all data privacy litigation.[43]

With the growth of Silicon Valley and the adjacent city of San Francisco as hotbeds of technological innovation, the concurrent rise in that technology's potential for privacy pitfalls opened the door for plaintiffs' firms. As far back as 2008, plaintiffs' lawyers such as the Lanier Law Firm of Texas were expanding to Silicon Valley to target intellectual property.[44] The Lanier firm, known for its asbestos and medical device litigation, soon expanded into privacy, suing Facebook in 2009 for alleged violations of its users' privacy in a suit that was quickly dismissed with prejudice.[45]

Since then, other firms have seized on the Bay Area and elsewhere in the Golden State as a liability destination, not only for its concentration of tech but also due to a number of plaintiff- and class action-friendly laws, including the Song-Beverly Credit Card Act (which prohibits businesses from collecting certain information from customers) and California's Unfair Competition Law (Business & Professions Code § 17200). Siprut PC opened a San Diego office in 2013, and KamberLaw expanded to California a few years ago.[46] In November 2015, Edelson PC announced that it would open a San Francisco office to allow it to more easily monitor what tech companies are doing and file cases.[47] Edelson filed 13 lawsuits in California state and federal courts in 2015, followed by 11 such lawsuits in 2016, which represent twice as much activity in those venues as before the move.[48]

> *"The district courts of California are where many of the privacy battles are being fought, accounting for one third of all data privacy litigation."*

Other privacy litigation hot spots include the Northern District of Illinois, accounting for 16 percent of privacy complaints filed in 2015, and where the Biometric Information Privacy Act and other consumer privacy-friendly laws have lured plaintiffs.[49] Also popular are the Eastern District of New York and the Eastern District of Wisconsin, which each accounted for six percent of privacy complaints filed in 2015.[50]

More broadly, privacy practice groups have been on the rise at law firms for several years, on both the plaintiff and defendant sides. According to a Bloomberg Law/International Association of Privacy Professionals study, 76 percent of corporations use outside counsel for privacy and data security matters.[51] Outside counsel play an important role in anticipating potential litigation; as described previously, between the third quarter of 2013 and the third quarter of 2014, 240 firms filed data privacy and security complaints.[52] When companies increase their legal arsenals, they are responding to the specter of lawsuits.

The activities of the AAJ, the national organization of plaintiffs' attorneys, also show increased focus on privacy. The AAJ has formed a specific consumer privacy/data litigation group, which is bringing together knowledge and documents from similar cases, identifying successful litigation strategies, and assembling a network of attorneys that consult with each other on privacy issues.[53] This collaboration aims to make privacy litigation accessible for more plaintiffs' firms.

"The AAJ has formed a specific consumer privacy/data litigation group, which is bringing together knowledge and documents from similar cases, identifying successful litigation strategies, and assembling a network of attorneys that consult with each other on privacy issues. This collaboration aims to make privacy litigation accessible for more plaintiffs' firms."

New Tactics of the Plaintiffs' Bar

Plaintiffs' law firms have come up with new strategies to fuel their class action factories. Companies must regularly fend off aggressive tactics ranging from taking advantage of regulatory reporting requirements to commissioning studies on vulnerabilities.

Exploiting Breach Notifications

Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have each created their own breach notification standards. Many of those laws require companies that have experienced data loss or exposure to report those breaches to affected individuals, the public, or the attorney general of that state or territory. These reporting requirements often apply even when there has been access to, but no theft of, data, and there is no risk of harm to those affected.[54] Numerous attorneys general, including those in California,[55] Washington,[56] and Iowa,[57] post a running public list on their websites of the data breaches that have been reported to them, including information provided by the companies regarding how many individuals in that state and/or nationally were affected.

Plaintiffs' firms use these required notifications as a roadmap to identify whom to sue. When breach notification letters are sent or the attorneys general provide a daily digest of the latest data incidents, all the lawyers must do is find a named plaintiff and cobble together a class action complaint from a template—their investigatory work has been done for them. It is widely apparent that attorneys are keeping close tabs on these notifications, particularly when complaints are sometimes filed within 24 hours of the announcement of a breach. As notable examples, after shoe retailer Zappos revealed that it had suffered a breach, a class action lawsuit was filed within a day.[58] When news of the Anthem breach broke, three class actions were filed within 24 hours.[59]

Investigating Potential Vulnerabilities

Not content with the cases reported in the news and revealed on attorney general websites, some firms have begun devoting significant resources to investigating

> *"Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have each created their own breach notification standards."*

> *When breach notification letters are sent or the attorneys general provide a daily digest of the latest data incidents, all the lawyers must do is find a named plaintiff and cobble together a class action complaint from a template—their investigatory work has been done for them.*

and creating class actions on their own. Edelson PC has a Case Development & Investigations Group, which the firm describes as investigating "complex technological fraud and privacy related violations, including fraudulent software and hardware, undisclosed tracking of online consumer activity, illegal data retention, and large-scale commercial data breaches," with the goal of creating cases.[60] In order to conduct its investigation of law firm security, Edelson uses its own laboratory of forensic engineers and lawyers.[61] One of the lab's goals is identifying vulnerabilities in products to target companies.[62]

The research of this forensics team has led to a number of lawsuits, including Edelson's August 2016 suit against the Golden State Warriors basketball team, which alleged that the team's app accessed phone microphones and recorded conversations without permission.[63]

Filing Complaints Under Seal

When Edelson filed its complaint against a Chicago law firm for security breaches, it filed under seal, a move that meant the law firm being sued received no notice of the suit until the case had been developed and strengthened. Under Federal Rule of Civil Procedure 5.2, a court may approve filing under seal without redaction, and may later unseal the filing.[64]

Jay Edelson told the press that the secret filing was necessary because "litigation provides a road map to hackers who are able to search dockets and identify redacted information that they think could be useful or valuable, then find out which law firms are involved and target those law firms to obtain the information."[65] He is now moving to unseal the complaint since the law firm has supposedly repaired its vulnerabilities. But the covert complaint has other advantages for the plaintiffs: Since the defendant has no notice of the filing, the case is well on its way to class certification before the defendant has an opportunity to prepare arguments and defend itself.

Targeting Statutory Damages

Identifying laws that provide statutory damages when a technical violation has occurred is one way plaintiffs' attorneys rack up a big payday simply by assembling a class. The TCPA, for example, automatically awards at least $500 for each phone call or text message that was placed or sent without meeting the law's stringent consent requirements, and that number

can be trebled to $1,500 in cases of willful violations. It is no wonder that TCPA litigation has become a cottage industry, especially since the damage award is per violating call or text, not per plaintiff.

Other laws offering statutory damages that have become attractive class action targets include the Song-Beverly Credit Card Act in California and the Fair and Accurate Credit Transactions Act (FACTA). Under the Song-Beverly Act, merchants that process credit cards can be subject to a $1,000 penalty for each transaction in violation of the Act, which includes requesting that the customer provide certain information, such as a zip code, during the transaction.[66] There is no limit to the number of penalties a merchant can face.[67] Under FACTA, merchants are prohibited from printing more than the last five digits of a credit card number on a receipt.[68] Damages for willful noncompliance are up to $1,000 per violation, also with no damage caps in class actions.[69]

Piggybacking on Sympathetic Academics and Advocacy Groups

Many legal academics are concerned that the law does not adequately protect people's privacy rights or provide for consumer redress. Advocacy groups such as the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation similarly support greater protections. The papers and platforms that they produce aid the plaintiffs' bar and others investigating purported violations, who are always looking for new theories and vulnerabilities. When law professor James Grimmelmann publicized how Facebook secretly performed research on users by manipulating the content they saw and their ensuing moods, he called on the Maryland attorney general to investigate the company.[70] EPIC also filed a complaint with the Federal Trade Commission (FTC),[71] and U.S. Senator Mark Warner then asked the FTC to conduct an investigation.[72] Advocacy groups and academics, such as Professor Paul Ohm, warned in 2008 of Internet Service Provider "deep packet inspection," which they likened to wiretapping and which they said threatened to invade the privacy of all who use them to access the Internet.[73] Online advertising company NebuAd put its web tracking technology on hold, and the plaintiffs' bar then targeted many Internet Service Providers that had used it, primarily accusing them of wiretapping in violation of the Electronic Communication Privacy Act.[74] While the claims ultimately failed in the courts, they nonetheless required defendants to mount a costly defense.[75]

"Under the Song-Beverly Act, merchants that process credit cards can be subject to a $1,000 penalty for each transaction in violation of the Act, which includes requesting that the customer provide information, such as a zip code, during the transaction."

Theories of Liability

Plaintiffs' lawyers use both standard and non-traditional theories of liability to bring their class action complaints. They push established boundaries to create new litigation opportunities over the collection and use of information in the ordinary course of business, not just when there has been a breach. Many of the cases described in this section are ongoing, but the outcomes of the resolved claims are noted where available.

Standard Theories of Liability

The federal district courts of California and the Northern District of Illinois, as well as select other courts around the country, have witnessed the evolution of plaintiffs' data privacy and security liability theories over the past several years. While some of the theories are new, traditional theories of liability from tort and contract law still underpin these lawsuits. Negligence, breach of fiduciary duty, and standard breach of contract often appear in these complaints. Courts have not always agreed that these theories apply to data and security breaches.

NEGLIGENCE

In its complaint against Toytalk, Inc. over the company's "Hello Barbie" toy, Lieff Cabraser alleged that the defendant was negligent in failing to take reasonable measures to prevent collection, storage, or sharing of nonconsensual recordings of children under the age of thirteen.[76] After the case was removed to federal court, plaintiffs dismissed the case with prejudice.[77] Similarly, when Edelson sued a tanning salon that scanned customers' fingerprints for identification purposes, even absent a data breach, the firm alleged that the defendant was negligent because it owed the plaintiffs a duty to exercise reasonable care in the collection and use of their biometric data, claiming it did not implement reasonable procedural safeguards around the collection and use of the data.[78] The case was settled for $1.5 million, of which the attorneys received $600,000.[79]

"They push established boundaries to create new litigation opportunities over the collection and use of information in the ordinary course of business, not just when there has been a breach."

BREACH OF FIDUCIARY DUTY

Edelson filed suit against health care benefits company Premera following a breach of consumers' confidential information, alleging breach of fiduciary duty. The suit claimed that because the defendant had placed itself in a position of trust when it sought the class members' information,[80] it was involved in the fiduciary relationship between doctors and their patients, and was acting in the fiduciary relationship of an insurer to its insured. Finally, Edelson claimed that the Health Insurance Portability and Accountability Act (HIPAA) also established a fiduciary relationship.[81] In August 2016, the court granted the defendant's motion to dismiss, holding that the relationship was not the type of relationship that has been considered fiduciary in character and that the plaintiffs had not alleged that they were induced to relax the care and vigilance they ordinarily would have exercised concerning their information.[82]

BREACH OF CONTRACT

When Cohen & Malad, LLP sued a healthcare company after a data breach that exposed patient information, it alleged breach of express contract because the defendant had a contractual obligation to maintain the security of class members' personal and medical information, as noted in the defendant's privacy policy.[83] The case is ongoing.

Novel Theories of Liability

Plaintiffs' lawyers are creating new models for their complaints, in part by applying old theories that traditionally address other wrongs. Courts have generally dismissed the most specious claims for procedural or jurisdictional reasons, but some claims alleging injury even in the absence of demonstrable harm, such as identity theft, are still being tested in the courts. Should these claims be successful, plaintiffs will find it easier to induce defendants to settle in order to avoid protracted litigation.

New Twists on Common Law Claims

Attorneys are putting new spins on traditional common law claims, including conversion, unjust enrichment, false light invasion of privacy, intrusion upon seclusion, and publication of private facts. These theories have yielded mixed results.

CONVERSION

The plaintiffs in *Fowles v. Anthem, Inc., et al.*, led by Lieff Cabraser, allege conversion, a common law tort that consists of a voluntary act by one person inconsistent with the ownership rights of another, historically involving chattels such as livestock.[84] The *Fowles* plaintiffs used conversion to sue after Chinese hackers targeted Anthem, stating in their complaint that plaintiffs' personal health information—their property—was interfered with.[85] Multidistrict litigation in this case is ongoing.

INTRUSION UPON SECLUSION

Edelson brought suit against Twitter in 2015 for "systematically intercepting, reading, and altering the private messages of its users without their knowledge or consent,"[86] alleging the tort of intrusion upon seclusion. This invasion of privacy tort involves one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, when that intrusion would be highly offensive to a reasonable person.[87] Common examples would be a physical trespass or the use of a zoom lens to photograph

> *The theory of unjust enrichment, when applied to data privacy and security actions, hinges on the claim that the product the customer purchased was less valuable than what was expected because they believed that adequate data security was included.*

someone in their home.[88] Edelson used this tort to sue Twitter for its automatic, algorithmic scanning of messages to alter hyperlinks within their text.[89] The plaintiff ultimately dropped the case, dismissing his own claims with prejudice.[90]

UNJUST ENRICHMENT

The theory of unjust enrichment, when applied to data privacy and security actions, hinges on the claim that the product the customer purchased was less valuable than what was expected because they believed that adequate data security was included. One of the first cases to test this theory in this context was *Resnick v. AvMed*. AvMed is a health insurance provider that lost two laptops containing the personal information of its customers, resulting in a few incidents of identity theft.[91] Edelson claimed that damages stemmed from the class members' overpayment for data protection services that the defendant failed to deliver.

This theory would allow plaintiffs to recover a portion of their insurance premiums whether or not they suffered actual identity theft. The unjust enrichment claim survived AvMed's motion to dismiss, with the court concluding that the plaintiffs had met their burden of showing that the defendant received a benefit from the plaintiffs (their monthly premiums) without paying fair value for it (implementing data management and security measures that industry standards require).[92] The plaintiffs ultimately received monetary payments as part of a $3 million settlement.[93]

No Harm and Theories of Injury

A major battleground of privacy litigation is what constitutes harm sufficient to confer standing to sue. Many courts have rejected the theory that plaintiffs who have merely had their information exposed without anything further have suffered a cognizable injury. But other courts have explored the nuanced results of a data breach, testing theories of whether spending money on identity protection, worrying about identity theft, or statutory violations are sufficient harm.

In *Spokeo, Inc. v. Robins*, the Supreme Court considered whether a plaintiff who has suffered no concrete harm had standing to sue based on a minor or technical statutory violation. The statute at issue, the federal Fair Credit Reporting Act, requires consumer credit agencies to take reasonable steps to ensure the accuracy of information they report about individuals. The Court's decision was expected to address how much or what type of harm is necessary to show an injury to one's privacy. The Court's May 2016 decision was not so clear. It held that while a mere

statutory violation was not sufficient to maintain standing, plaintiffs could use an alleged statutory violation to prop up their actions as long as a tangible or intangible concrete injury supported the claim. The case was remanded to the Ninth Circuit to examine the "concreteness" of the harm.[94]

The implications of the ruling were immediately uncertain. Jay Edelson claimed victory, but he admitted that the decision was "almost impenetrable."[95] Contrary to Edelson's assertions, courts have already started using *Spokeo* to dismiss claims for failure to show concrete injury.[96] Scores of cases were stayed pending the outcome, and some of those courts now appear to be interpreting the Supreme Court's decision as establishing standards that plaintiffs must meet for their claims to survive. If *Spokeo* makes it more difficult for privacy plaintiffs to find success in federal courts, it could shift some of the weight of litigation from federal to state courts.

While many courts have rejected the assertion that spending money on identity theft protection and insurance or replacement card fees is cognizable harm sufficient for standing,[97] a few have accepted the theory. In 2011, the First Circuit held in *Anderson v. Hannaford* that the plaintiffs' claims for these expenses "involve actual financial losses from credit and debit card misuse. Under Maine contract law, these financial losses are recoverable as mitigation damages so long as they are reasonable."[98] Coming before the Supreme Court's 2013 decision in *Clapper v. Amnesty International*, which established the "actual injury" requirement for standing, it was unclear whether the *Anderson* case was still viable. But the Seventh Circuit held in the Neiman Marcus data breach case in 2015, after *Clapper*, that the preventive costs that credit card holders might incur following the breach of their credit card information easily qualify as concrete injuries.[99] In so ruling, the Seventh Circuit reversed a lower court, stating that identity fraud is a foreseeable consequence of a data breach, and the plaintiffs had standing to bring claims over the time and cost taken to prevent such fraud.[100]

> *"It is possible that if federal courts become overall more hostile to flimsy claims of harm, plaintiffs' firms, already forum-shopping among federal courts, may find that their next frontier is in state courts."*

Following the *Spokeo* decision, it is an open question how most courts will interpret the requirement of harm. So far, many district courts and circuit courts of appeal have ruled on both sides of the issue in cases involving technical violations of statutes, such as the TCPA and the Fair and Accurate Credit Transactions Act.[101] The Seventh Circuit remains an outlier in its recognition of non-identity theft harm. It is possible that if federal courts become overall more hostile to flimsy claims of harm, plaintiffs' firms, already forum-shopping among federal courts, may find that their next frontier is in state courts.

Old and Vague Laws Applied to New Problems

While states have hurried to pass a wide array of laws on data breach, plaintiffs' lawyers still continually seek additional avenues of statutory liability. They have sought to stretch existing laws, originally designed for other purposes, to extend to today's privacy landscape. The result is an often unpredictable application of laws which were never intended to cover the claims alleged.

Vague laws targeting unfair and deceptive acts and practices in trade (UDAP), both at the federal and state levels, have long been exploited to prosecute a multitude of offenses, whether at the hands of regulators or plaintiffs' lawyers. These UDAP laws often are so broad that they may encompass security practices that exposed a company to a data breach, lack of adherence to a privacy policy, or the sharing of information that was not disclosed to consumers. Given the rise of UDAP actions brought by the Federal Trade Commission, state attorneys general, and private plaintiffs, companies are now on notice that such laws pose a risk, but there is little that a company can specifically do to prepare.

"Vague laws targeting unfair and deceptive acts and practices in trade (UDAP), both at the federal and state levels, have long been exploited to prosecute a multitude of offenses, whether at the hands of regulators or plaintiffs' lawyers."

Old privacy laws intended to apply only to certain types of violations are also now fodder for plaintiffs' lawyers. The Video Privacy Protection Act (VPPA), passed in 1988 to protect video rental histories after U.S. Supreme Court nominee Robert Bork's rental list was published, is now regularly used to target video streaming services, such as Netflix and Hulu. It is especially attractive to plaintiffs because it provides for statutory damages of $2,500 per violation, with no cap on damages.[102] Hulu was sued under the VPPA for sharing user information with Facebook,[103] and Netflix was sued first in 2011 for retaining subscribers' information after they discontinued the service, and in 2012 for showing a subscriber's viewing queue and recommendation list on televisions connected to the subscriber's account.[104] After significant litigation, the court in the Hulu case granted summary judgment to Hulu.[105] Netflix settled the first VPPA case, but had the claims dismissed in the second case.[106]

Similarly, the Driver's Privacy Protection Act (DPPA), which also provides for $2,500 in statutory damages,[107] was passed in 1994 to protect against stalkers looking up addresses in public driver's license databases and harassing victims. In 2015, a former Coca-Cola employee sued the

> *"[T]oday, plaintiffs routinely use the CFAA to allege that defendants have accessed their information and invaded their privacy by engaging in practices such as placing cookies on browsers to track online activity for advertising purposes."*

company under the DPPA, alleging that the compromise of information about the company's drivers when laptops were stolen from the company constituted a violation of the law.[108] A Pennsylvania district court dismissed the plaintiff's DPPA claim because Coca-Cola had not knowingly given out his driver's license information.[109]

Finally, the Computer Fraud and Abuse Act (CFAA) was enacted as a criminal statute in 1986 to combat hacking, with a private civil right of action added in 1994.[110] The law prohibits accessing computers or exceeding permitted access to obtain information, such as a hacker would.[111] But today, plaintiffs routinely use the CFAA to allege that defendants have accessed their information and invaded their privacy by engaging in practices such as placing cookies on browsers to track online activity for advertising purposes. These claims are often dismissed.[112]

Specious Claims

Plaintiffs' firms are creatively manufacturing legal theories to make companies pay for supposed privacy violations. The resulting specious claims have met with some success in the courts, despite their lack of foundation in case law.

Some claims are based on privacy policies and privacy statements that are not necessarily part of a contract. In *Dolmage v. Combined Ins. Co. of Am.*, a "Privacy Pledge" document was included in insurance policy papers provided to employees of Dillard's, similar to "privacy statements" that consumers receive from banks and credit card issuers. The pledge stated that the insurance company used certain safeguards to protect policyholders' information.[113] After a third-party vendor used an insecure method of data storage, potentially exposing the policyholders' personal information, the plaintiffs defeated a motion to dismiss their suit by successfully arguing that the "Privacy Pledge" was part of the policy obtained from the insurer.

Other claims are based on the reading of implied promises in contracts. Under the theory of breach of implied contract, when a contract obligates someone to hand over their personal information, there is an implicit promise that the information will

be reasonably safeguarded and will only be used for the purposes for which it was collected. In its suit against Sony, Lieff Cabraser claimed that Sony had breached an implied contract because, in order to receive compensation and other employment benefits, Sony required employees to provide their personal information, including names, addresses, Social Security numbers, and medical information. Thus, plaintiffs claimed that Sony had an implied duty of good faith to ensure that the personally identifiable information about plaintiffs in its possession was only used to provide employee compensation and other employee benefits.[114] It did not matter to plaintiffs that Sony was the victim of a North Korean hacking attack. In October 2015, Sony reached an $8 million settlement with the class, agreeing to reimburse employees for losses and harm.[115]

Plaintiffs have also sought to hold corporate directors and officers accountable for breaches, claiming that they breached their fiduciary duties or committed corporate waste by not adequately protecting the company's cybersecurity. The 1996 *Caremark* decision by the Delaware Chancery Court held that directors can be held personally liable for failing to appropriately monitor and supervise the enterprise.[116] Plaintiffs can base shareholder derivative suits on the fallout from data breaches by alleging that such inattention led to government enforcement, fines, and declining share prices. Shareholders sued Target following its data breach, as did shareholders of Wyndham Worldwide, when it experienced a breach. These suits have proven unsuccessful in the courts.[117]

Preventing Exploitation of Privacy and Data Security

Although some attempts to stretch legal theories have failed, attempts to recover for data breaches through class action litigation will certainly not cease. Companies must pay to defend even specious claims, deploying needless financial and personnel resources, racking up costs that ultimately hurt shareholders, employees and consumers.

Legal reforms can help stem this tide of litigation by considering how plaintiffs are abusing the system and whether there should be a more comprehensive regulatory scheme that provides predictability for companies, as well as protection for consumers and citizens.

Harmonize Notification Laws

First, notification laws should be harmonized. Currently, the complicated patchwork of state laws on privacy and data breach works to plaintiffs' advantage. When nearly every state has a different law, the compliance burden on companies is very heavy—such as when they must quickly notify customers of a breach—and plaintiffs are swift to call attention to any omissions. A federal data breach notification law that preempts the patchwork of state laws would streamline the compliance burden.

Require Risk Analysis

Second, including a risk-of-harm analysis in state breach laws would address plaintiffs' exploitation of vulnerabilities. Requiring notification of a data breach only when people are actually at risk of harm would reduce excessive notifications, which plaintiffs rely on to bring cases. Plaintiffs' lawyers closely monitor attorney general websites for breach notifications and

"A federal data breach notification law that preempts the patchwork of state laws would streamline the compliance burden."

are also alerted when companies send consumer notification letters. When breach notification is required, even when no one has been harmed or is at risk of harm, plaintiffs' lawyers are handed lawsuits on a silver platter. Some states have such laws in place, and wider adoption of comparable risk analysis provisions would significantly reduce reporting requirements and no-harm lawsuits.

Limit Abusive Litigation

Finally, a reform framework is also needed to limit abusive litigation. Reforms could address the proportionality of attorneys' fees; disallow statutory penalties without proof of harm; provide that meeting defined compliance standards would bar private rights of action absent gross misconduct; and impose damage caps on penalties. None of these provisions would eliminate the ability of aggrieved plaintiffs to sue violators. Instead, these reforms would impose a rational and predictable set of standards that, among other things, would ensure that only those who are truly injured may recover—a longstanding principle of American tort law. They would also ensure that compensation is proportional to injury and that lawyers do not benefit at the expense of their clients.

Some reforms are already before state legislatures. For example, a compliance safe harbor would provide companies with certainty and peace of mind against data breach lawsuits as long as they met a certain standard of security. Such a safe harbor, similar to that proposed in New York,[118] would allow immunity from public and private lawsuits as long as companies certify their compliance with prescribed standards and do not commit gross negligence or willful misconduct.

> *"[Reforms] would impose a rational and predictable set of standards that, among other things, would ensure that only those who are truly injured may recover—a longstanding principle of American tort law."*

Addressing issues such as these will help halt the expansion of liability before it spirals out of control. The skyrocketing costs of contending with a data breach should not be exacerbated by opportunistic plaintiffs' lawyers who engineer liability claims for their own profit in the absence of real damage.

Endnotes

1 Bryan Cave, "2015 Data Privacy Litigation Report" at 3 (May 2015) available at http://www.bryancavedatamatters.com.

2 *See* BTI Consulting Group, "BTI Business Development Opportunity Zones" (Nov. 2015), available at http://www.bticonsulting.com/how-to-grow-your-law-firm.

3 *See* IBM and Ponemon Institute LLC, "2016 Cost of Data Breach Study: United States" (June 2016), available at www.ibm.com/security/data-breach.

4 *See* "2015 Data Privacy Litigation Report," *supra* at 10.

5 "Litigation Groups," American Association for Justice, available at https://www.justice.org/membership/litigation-groups.

6 *See* Adam Liptak, "When Lawyers Cut Their Clients Out of the Deal," New York Times (Aug. 12, 2013).

7 *See id.*

8 *See* Ahiza Garcia, "Target Settles for $39 Million Over Data Breach," CNN (Dec. 2, 2015).

9 *See In re: Target Corp. Customer Data Security Breach Litigation*, MDL No. 2522 (D. Minn. 2014).

10 *See* Emily Field, "Target's $10M Data Breach Deal Survives 8th Circ. Appeal," Law360 (Jan. 27, 2016).

11 *See* Edvard Pettersson, "Sony to Pay as Much as $8 Million to Settle Data-Breach Case," Bloomberg Technology (Oct. 20, 2015).

12 *See id.*

13 *See* Jonathan Stempel, "Home Depot Settles Consumer Lawsuit Over Big 2014 Data Breach," Reuters (Mar. 8, 2016).

14 *See* Maria Halkias, "Neiman Marcus to Pay $1.6 Million in Shopper Data Breach Lawsuit," Dallas News (Mar. 20, 2017).

15 *See* Jeremy Kirk, "Premera, Anthem Data Breaches Linked By Similar Hacking Tactics," Computerworld.com (Mar. 18, 2015).

16 *See* Steven Trader, "Anthem Hit With Suit Over Massive Health Data Breach," Law360 (June 29, 2015).

17 *See* Jonathan Vanian, "IRS Sued Over Data Breach That Affected 330,000 People," Fortune (Aug. 21, 2015).

18 *See* Steven Trader, "IRS Wants Data Breach Suit Tossed For Lack Of Standing," Law360 (Feb. 4, 2016).

19 *See Spokeo, Inc. v. Robins*, available at http://www.supremecourt.gov/opinions/15pdf/13-1339_f2q3.pdf.

20 *See* Debra Cassens Weiss, "Netflix Notifies Customers of Class Action Settlement; Privacy Groups Will Benefit," ABA Journal (Aug. 1, 2012).

21 *See* "2015 Data Privacy Litigation Report," *supra* at 7.

22 "Block Calls Get Cash," www.blockcallsgetcash.com.

23 Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*

24 Stephanie N. Grimoldby, "Logging in: Growing Class Actions Use IL Biometric Privacy Law To Target Social Media Titans, Many Others," Cook County Record (Jul. 6, 2016).

25 *See id.*

26 *See* Alaska Genetic Privacy Act, AS § 18.13.010-100.

27 *See* Kyla Asbury, "Alaska Class Action Lawsuit Says Family Tree DNA Posted Info on Public Websites," Legal NewsLine (May 16, 2014).

28 *See id.*

29 Conor Dougherty, "Jay Edelson, the Class-Action Lawyer Who May Be Tech's Least Friended Man," New York Times (Apr. 4, 2015).

30 *See id.*

31 Gabe Friedman, "Threats of Litigation After Data Breaches at Major Law Firms," Bloomberg Law (Mar. 30, 2016).

32 *See id.*

33 Allison Grande, "Edelson Targets Chicago Law Firm Over Lax Data Security," Law360 (May 5, 2016).

34 *See* Roy Strom, "Chicago's Johnson & Bell First US Firm Publicly Named in Data Security Class Action," The American Lawyer (Dec. 9, 2016).

35 *Id.*

36 *See* Dougherty, *supra*.

37 Based on docket research.

38 Based on docket research.

39 *See* Jessica Guynn, "Facebook to Face Privacy Lawsuit Over Photo Tagging," USA Today (May 6, 2016).

40 *See* Lance Duroni, "Walgreen Asks 8th Circ. To Settle Tracking Suit Venue Feud," Law360 (June 4, 2013).

41 *See* Adam Liptak, "When Lawyers Cut Their Clients Out of the Deal," New York Times (Aug. 12, 2013).

42 *See id.*

43 *See* "2015 Data Privacy Litigation Report," *supra* at 3.

44 *See* Zusha Elinson, "Texas' Lanier Law Firm Opens IP Office in Silicon Valley," The American Lawyer (Apr. 1, 2008).

45 *See* Ashby Jones, "Mark Lanier's Latest Target: Facebook," The Wall Street Journal Law Blog (Aug. 18, 2009).

46 *See* Allison Grande, "Privacy Class Action Growth Fuels New California Gold Rush," Law360 (Nov. 5, 2015).

47 *See* Allison Grande, "Plaintiffs Firm Edelson Brings Privacy Prowess to SF," Law360 (Nov. 4, 2015).

48 *See* Ross Todd, "Novel Suits, Setbacks Mark Edelson's First Year in Calif.," The Recorder (Jan. 9, 2017).

49 *See* "2015 Data Privacy Litigation Report," *supra* at 4.

50 *See id.*

51 "The Market for Privacy Legal Services," Bloomberg Law and the International Association of Privacy Professionals (Apr. 5, 2016).

52 *See* "2015 Data Privacy Litigation Report," *supra* at 10.

53 "Litigation Groups," American Association for Justice, available at https://www.justice.org/membership/litigation-groups.

54 *See, e.g.*, the laws of Connecticut, New Jersey, and Puerto Rico, which trigger notification when data is merely accessed.

55 "Search Data Security Breaches," State of California Department of Justice Office of the Attorney General, available at https://oag.ca.gov/ecrime/databreach/list.

56 "Data Breach Notifications," Washington State Office of the Attorney General, available at http://www.atg.wa.gov/data-breach-notifications.

57 "Security Breach Notifications," Iowa Department of Justice Office of the Attorney General, available at https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/.

58 *See In re: Zappos.com Inc. Customer Data Security Breach Litigation*, MDL number 2357 (D. Nev.).

59 *See In re Anthem, Inc. Data Breach Litigation*, No. 5:15-md-02617 (N.D. Cal. 2015).

60 "Christopher L. Dore," Edelson, available at https://www.edelson.com/team/christopher-l-dore.

61 Grande, "Edelson Targets Chicago Law Firm," *supra*.

62 *See id.*

63 *See* Todd, *supra*.

64 F.R.C.P. 5.2(d).

65 Grande, "Edelson Targets Chicago Law Firm," *supra* (internal citations omitted).

66 *See* Cal. Civ. Code §§ 1747.1, 1747.08.

67 *See id.*

68 *See* 15 U.S.C. § 1681c.

69 *See* 15 U.S.C. § 1681n.

70 *See* James Grimmelmann, "Illegal, Immoral, and Mood-Altering: How Facebook and OKCupid Broke the Law When They Experimented on Users," Medium.com (Sept. 23, 2014).

71 *See* "In re: Facebook (Psychological Study)," Epic.org, available at https://epic.org/privacy/internet/ftc/facebook/psycho.

72 *See* Gregory S. McNeal, "Did Facebook Break The Law? Senator Asks FTC for Answers," Forbes (July 9, 2014).

73 *See* Paul Ohm, "The Rise and Fall of Invasive ISP Surveillance," U. Ill. L. Rev. (2009).

74 *See* Steven A. Augustino and Barbara A. Miller, "Court rules for ISP in deep packet inspection lawsuit," Lexology.com (Jan. 7, 2013).

75 *See id.*

76 *See Archer-Hayes v. Toytalk, Inc.*, No. 2:16-cv-02111 (C.D. Cal. 2016).

77 *See id.*

78 *See Sekura v. Krishna Tan, Inc., et al.* (Ill. Cir. Ct. 2016).

79 *See* Jonathan Bilyk, "L.a. Tan Settles Fingerprint Scan Privacy Class Action for $1.5M; Attorneys Get $600K," Cook County Record (Dec. 9, 2016).

80 *See In Re Premera Blue Cross Customer Data Security Breach Litigation*, No. 3:15-md-02633 (D. Or. 2015).

81 *See id.*

82 *See id.*

83 *See In Re: Medical Informatics Engineering, Inc., Customer Data Security Breach Litigation*, No. 3:15-md-02667 (N.D. Ind. 2015).

84 *See* Restatement (Second) of Torts § 222A.

85 *Fowles v. Anthem, Inc., et al.* 5:15-cv-02249 (N.D. Cal. 2015).

86 *Raney v. Twitter*, No. 3:15-cv-04191 (ND Cal. Sept. 14, 2015).

87 Restatement (Second) of Torts § 625B.

88 *See Id.*

89 *See Raney*, No. 3:15-cv-04191.

90 *See* Jody Godoy, "Twitter User Drops Direct Messaging Privacy Suit," Law360 (Jan. 19, 2016).

91 *Resnick v. AvMed*, 693 F.3d 1317 (11th Cir. 2012).

92 *Resnick*, 693 F.3d at 1328.

93 *See Resnick v. AvMed*, No. 10-cv-24513, Dkts. 82, 91 (S.D. Fla. October 25, 2013); Allison Grande, "AvMed's $3M Pact Blazes New Path for Data Breach Settlements," Law360 (Oct. 28, 2013).

94 *See Spokeo*, *supra*.

95 Allison Grande, "Spokeo Ruling Helps Both Sides Of Privacy Bar, Attys Say," Law360 (May 25, 2016).

96 *See, e.g., Sandoval v. Pharmacare US, Inc.*, No. 15-cv-0738-H-JLB (S.D. Cal. 2016).

97 *See, e.g., Randolph v. ING Life Insurance and Annuity Co.*, 486 F. Supp. 2d (D.D.C. 2007).

98 *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 167 (1st Cir. 2011).

99 *Remijas v. Neiman Marcus Group, LLC*, No. 14-3122 (7th Cir. 2015)

100 *See id.*

101 *See, e.g., Cruper-Weinmann v. Paris Baguette America Inc.*, No. 1:13-cv-07013 (S.D.N.Y. Jan. 31, 2017); *Bradley Van Patten v. Vertical Fitness Group et al.*, No. 14-55980 (9th Cir. 2017).

102 *See* 18 U.S.C. § 2710(c).

103 *See* Caleb Skeath, "Court Grants Summary Judgment on VPPA Claims Against Hulu Based on Lack of 'Knowing' Disclosure," The National Law Review (Apr. 13, 2015).

104 *See* Jeff Roberts, "Update: Netflix Pays $9 Million to Settle Video Privacy Lawsuit," Gigaom (Feb. 10, 2012); Venkat Balasubramani, "9th Circuit Rejects VPPA Claims Against Netflix For Intra-Household Disclosures," Technology & Marketing Law Blog (July 31, 2015).

105 *See* Skeath, *supra*.

106 *See* Roberts, *supra*; Balasubramani, *supra*.

107 *See* 18 U.S.C. § 2724(b)(1).

108 *See* Jody Godoy, "Coca-Cola Gets Worker's Data Breach Suit Trimmed," Law360 (Oct. 1, 2015).

109 *See id.*

110 *See* 18 U.S.C. § 1030(g).

111 *See* 18 U.S.C. § 1030.

112 *See, e.g., In Re: Specific Media Flash Cookie Litig.*, No. 8:10-cv-01256 (C.D. Cal. 2010).

113 *Dolmage v. Combined Ins. Co. of Am.*, No. 1:14-cv-3089 (N.D. Ill. Feb. 23, 2016).

114 *See Corona, et al. v. Sony Pictures Corp.*, No. 2:14-cv-09600 (C.D. Cal. 2015).

115 "Sony Data Breach," Lieff Cabraser, available at http://www.lieffcabraser.com/privacy/sony-data-breach.

116 *See In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 971 (Del. Ch. 1996).

117 *See Mary Davis et al. v. Gregg W. Steinhafel et al.*, No. 0:14-cv-00203 (D. Minn. 2014); *Dennis Palkon et al. v. Stephen P. Holmes et al.*, No. 2:14-cv-01234 (D. N.J. 2014).

118 See New York State Assembly Bill A06866, available at http://assembly.state.ny.us/leg/?default_fld=&bn=A06866&term=2015&Summary=Y&Actions=Y&Text=Y. Companies certified as client shall be immune from liability in a civil action, including but not limited to an action brought by the attorney general, resulting from unauthorized access to private information by a third-party absent evidence of willful misconduct, bad faith or gross negligence. Compliance must be certified annually by an independent, third-party licensed insurer, authorized by NIST.

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com