73 Consumer Fin. L.Q. Rep. 6

Consumer Finance Law Quarterly Report
2019

J.H. Jennifer Lee [a1] Kimberly B. Frumkin [a2] Susan Tran [a3] Nicolás Sánchez-Mandery [a4]

CONSUMER PROTECTION IN THE NEW ECONOMY: *PRIVACY CASES IN E-COMMERCE TRANSACTIONS OR SOCIAL MEDIA ACTIVITIES*

I. INTRODUCTION

This article examines litigation trends related to Internet commerce and consumer protection arising in the context of privacy. We focus on the evolution of legal standards, as manifest in judicial decisions nationwide. Internet-based commerce is ubiquitous, and it is reasonable to expect that as "Big Data" and the use of consumers' information becomes more pervasive, ***7** public policy concerns, pioneering technologies, and customer expectations may conflict. This issue impacts several industries nationwide, including data aggregators, retailers, financial services firms, social media platforms, and manufacturers of consumer goods (smart TVs, etc.). Assessing past litigation and other legal trends in this space--which we discuss herein--can permit businesses to be better prepared for the future and regulators to develop new privacy rules (including the new California privacy law enacted June 2018) in a manner that is rational within a larger context. In addition, a deep dive into the legal precedents decided, to date, helps to inform policymaking by elected officials and state or federal legislators.

We begin our discussion by framing the question. On the one hand, the proliferation of Internet technology has improved the speed, convenience, and ability of consumers to locate, compare, and buy products and services online. On the other hand, many of these conveniences often come with tracking, storing, and sharing of what some consumers view as their private information, including for example, content viewing history. In these instances during which a consumer believes she has been aggrieved by corporate conduct as relating to her individual privacy rights, conventional wisdom suggests that such a consumer could vindicate her rights in court. Can she?

It depends. As courts have grappled with applying existing litigation procedures and substantive privacy standards to new technology, we have identified four major categories where privacy concerns have arisen within the consumer-protection framework: 1) a specific trend of legal cases targeting companies with an Internet presence in the absence of any data breach that consumers have brought thus far in court; 2) whether the injury-in-fact requirement poses an obstacle to plaintiffs establishing claims; 3) the ability to prevail when data-security services were not part of the bargain at hand; and 4) the monetary value of one's personal data. In addition, it is illuminating to consider 5) social science research on whether consumers even care about privacy. Each of the foregoing items is explained in further detail below. We conclude that because of procedural complexities in litigation and the ad-hoc, case-by-case approach taken by courts, privacy is an area that is ripe for additional claims as plaintiffs become increasingly well-versed in data and consumer rights, aided by new privacy laws coming into effect in future years.

II. PLAINTIFFS TARGET SOCIAL MEDIA COMPANIES, RETAILERS, OR CONSUMER-FACING BUSINESSES, EVEN IN THE ABSENCE OF A DATA BREACH

While much public attention recently has been focused on data-protection issues in the context of a data breach or malicious hacks, a more provocative fact pattern--for purposes of assessing substantive "consumer rights" in the new economy--arises in

court cases alleging liability in the absence ***8** of a data breach. [1] Generally, such cases involve the following alleged facts: plaintiffs took steps to keep their user data private by employing certain software or opt-out mechanisms to disallow the use of cookies by websites; defendants circumvented such mechanisms by allegedly "exploiting" known loopholes, managing to place cookies on the plaintiffs' computers against their wishes; this conduct resulted in the plaintiffs' loss of their privacy in their web browsing history and a gain to defendants, who would be able to use the plaintiffs' browsing history to deliver targeted ads and otherwise aggregate the data into an economically valuable commodity. [2]

As "Big Data," tools like Alexa and Google Home, retail subscription services, data aggregators for personal financial planning, or the Internet of Things continue to proliferate in the new economy, consumers and market participants will inevitably engage in new kinds of data-sharing or data-use transactions. The case law discussed herein provides an interesting landscape for the types of dispute that may arise in the future, because such new products and services all entail new forms of use of consumers' private information.

What is notable about past cases is that they reveal the absence of a single, "one size fits all," regulation or statutory provision that sets forth a private right of action in the absence of a data breach, relating to retailers' or online social media platforms' use of consumers' data. [3] Accordingly, ***9** plaintiffs have used a multi-faceted approach to privacy claims, asserting a panoply of federal or state statutory violations and common law claims. Below, we summarize a few such cases in more detail.

Internet advertising companies have faced litigation regarding the alleged practice of surreptitiously placing third-party cookies on web users' computers in order to show users targeted advertisements. [4] One such complaint alleged that the defendants used code to exploit a loophole in certain Internet browsing software to enable them to place third-party cookies on web users' computers, despite the users having set their browser settings to reject such cookies. [5] The multi-district litigation was consolidated and presented as a putative class action, with plaintiffs alleging that the defendants violated the Federal Wiretap Act, the Store Communications Act (SCA), and the Computer Fraud and Abuse Act (CFAA). Google also faced six California state law claim violations under California's Unfair Competition Law, the California Comprehensive Computer Data Access and Fraud Act, the California Invasion of Privacy Act (CIPA), the California Consumers Legal Remedies Act (CLRA), as well as violations of users' privacy rights under the state's constitution and intrusion upon seclusion under California law. The Third Circuit affirmed the district court's decision to grant dismissal of all the claims against defendants for failure to state a claim, other than for the privacy claim under the California constitution. [6] After the decision from the Third Circuit, the parties engaged in private mediation efforts, which were successful.

In 2012, users of a social media company brought a multi-district class action against the company over specific, alleged tracking practices that are unique to e-commerce or social media activity. In that case, the plaintiffs sought over $15 billion in damages and injunctive relief for "knowing interception of users' internet communications and activity" after users had ***10** logged out of their accounts. [7] As to the technology, the plaintiffs alleged that the company was tracking and storing their post-logout internet usage activity using small text files that had been embedded in their computer's browsers. [8] After the court dismissed these initial claims, in some cases for failure to show standing, and in others for failure to state a claim, the plaintiffs brought an amended complaint. [9] The court again dismissed these claims for failure to establish standing and failure to state a claim, putting an end to the six-year litigation. [10]

While the series of social media and e-commerce cases have focused on substantive technologies involving tracking data or content viewing histories, a key issue from a legal standpoint that weaves through every case is standing to sue.

III. THE INJURY-IN-FACT DEBATE: IS LOSS OF PRIVACY AN AMORPHOUS HARM?

A threshold issue any consumer must overcome in court is whether she has standing to sue. Litigants address this issue head-on when defendants lodge, procedurally, a motion to dismiss for lack of jurisdiction or for failure to state a claim for which

relief can be granted. The standing question is a constitutional requirement that applies with different standards depending on whether the case is in federal or state court.

In the context of prior litigation on privacy matters, a case will live or die based on the consumer's ability to demonstrate standing. To satisfy standing in federal court, one must demonstrate that she suffered an "injury in fact," or an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, and not conjectural or hypothetical, and that (c) the injury is "fairly traceable to the challenged action of the defendant," and (d) it is "likely, as opposed to merely speculative, that the injury will be redressed" if the court issues a favorable decision. [11]

While the seminal Supreme Court case on standing, *Spokeo, Inc. v. Robins*, [12] has further bolstered the necessity for plaintiffs to show "concrete" ***11** and "particularized" harm, court decisions pre-dating *Spokeo* have evinced a trend whereby plaintiffs must show actual harm in privacy cases, or else face dismissal under Federal Rule of Procedure 12(b)(1) or 12(b)(6). This requirement is also found in state law, as "[t]he purpose of the standing doctrine is to ensure that litigation is brought only by the appropriate parties having a present, substantial interest in the outcome ...., as well as to prevent parties from '[c]reating controversies in matters in which they are not involved and which do not directly affect them.'" [13] The requirement is particularly thorny in situations where plaintiffs assert a privacy violation but have not really suffered from a data breach.

As the Supreme Court made clear in *Spokeo*, while an injury to show Article III standing must be "concrete," meaning "real, and not abstract," this does not mean that the injury must be tangible to be real. [14] Intangible injuries, however, which predominate in privacy litigation, are often more difficult to recognize than the tangible variety. [15]

As to the standing issue, in the last twenty years, we have seen a mixed bag of results in the privacy context, which are generally dependent on how well the plaintiff pleads the facts, the jurisdiction in which the plaintiff chooses to bring the case, and other factors. One significant factor in whether or not plaintiffs will be able to make out standing has to do with the types of claims the plaintiffs allege. The type of claim brought will dictate the type of injury a plaintiff must show, and whether such injury must be tangible, or if an intangible injury will suffice. Even for those claims for which an intangible injury is sufficient, given the circumstances that are typically present when plaintiffs file their claims, plaintiffs in privacy lawsuits face an uphill battle to demonstrate that the injury is sufficiently real to allow the claims to proceed past the motion to dismiss stage.

These issues include: laws that require a tangible loss to proceed in court; consumers' relatively inferior knowledge concerning the monetization of their personal data; the impact that cookies are alleged to have on device performance; and the stratification of services offered in terms of retailers/social media platforms vs. security services firms. We elaborate on each such issue below.

A. Tangible Loss Arguments.

A number of common claims brought by plaintiffs in these cases require a tangible injury. [16] These claims include alleged violations of the CFAA, [17] ***12** trespass to chattels, [18] fraud, larceny, [19] and conversion. [20] Even in the absence of these specific claims, some plaintiffs, especially when privacy tracking claims were first brought, claimed the injury plaintiffs suffered was in the nature of economic harm, instead of attempting to show an intangible injury that may have had more success. [21]

Plaintiffs who attempt to show a concrete and particularized injury based on pecuniary loss often attempt to make three arguments: (1) that plaintiffs' personal browsing history is a valuable commodity which defendants took without authorization, (2) that the placement of cookies on their devices diminished the performance of said devices, and (3) that defendants' privacy policies promised not to share personal information, and by doing so, plaintiff did not receive the full benefit of the paid for services, resulting in economic harm.

1. ***Browsing history as a valuable commodity.***

That plaintiffs' personal browsing history has intrinsic value is a notion which courts usually accept. Instead, arguments predicated on the inherent value of browsing history have failed because plaintiffs are unable to show how defendants' collection and use of plaintiffs' browsing history diminishes or forecloses plaintiffs also monetizing their tracking history. For instance, in *LaCourt v. Specific Media, Inc.*,[22] the plaintiffs asserted that the defendants circumvented their privacy and security controls to place cookies ***13** on plaintiffs' computers to track their web browsing history, causing economic loss to plaintiffs. The economic loss argument was premised on the allegation that their personal browsing history had discernable value, which plaintiffs were deprived of when defendant used it for its own personal benefit.[23] However, the court found that plaintiffs did not show that any of the litigants actually ascribed an economic value to their browsing history, as none of them had ever attempted to sell such data. Moreover, the court found that "Plaintiffs [did] not explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party."[24]

In a prior case involving a social media company, plaintiffs encountered a similar barrier. After surveying similar cases, including *LaCourt*, that court reached the same conclusion--that plaintiffs had not shown, for purposes of Article III standing, that the value of their information was somehow diminished after it was collected by the third party company.[25] The court's conclusion in this regard was not altered by the fact that the plaintiffs had alleged a limited marketplace in which plaintiffs could sell their browsing data, as there was still no showing that defendant's collection of browsing data impacted plaintiffs' ability to sell the data as well.[26]

Moreover, litigants bringing a recent case in the Southern District of New York unsuccessfully tried to put a different spin on this argument in an attempt to sidestep the necessity of showing how the defendant's use of the data resulted in an economic loss to plaintiffs. In *Mount v. PulsePoint, Inc.*,[27] the plaintiffs argued that they did not need to plead that their ability to monetize their data was diminished, as the fact that it was misappropriated was enough. In making this argument, plaintiffs attempted to compare the misappropriation of their browsing history to cases involving misappropriation of confidential business information.[28] The court rejected this argument, finding such cases to be inapposite. In doing so, the court noted that the plaintiffs in *PulsePoint* did not assert a property right in the exclusive use of their browsing information. Moreover, the court noted that in confidential business information cases, the "exclusive use of the information was critical to its commercial value to the plaintiff businesses, and unauthorized disclosure to others risked harming the plaintiffs' ability to capitalize on that value."[29] However, in a ruling that echoed *LaCourt* and similar cases, the court concluded that plaintiffs had made no argument ***14** as to why the collecting and sharing of browsing information would have a similar effect.

2. ***Diminished capabilities of devices with cookies.***

The second argument, that the placement of cookies on plaintiffs' computers constitutes a concrete and particularized injury, has seen mixed results. For example, in *LaCourt*, the court noted that "[i]f the loss of the ability to delete cookies counts as harm to Plaintiffs' computers, then maybe Plaintiffs have alleged some *de minimis* injury, but probably not one that would give rise to Article III standing" without alleging additional concrete facts showing how the computers were specifically impacted.[30] However, in *PulsePoint*, that court came to a different conclusion. Plaintiffs there likewise contended that the placement of cookies on their computer affected their devices. Although the court concluded that "plaintiffs have failed to allege any significant level of consumption of device capacity or any discernible interference with device performance, we believe that PulsePoint's alleged unauthorized setting of cookies on plaintiffs' devices is itself injury in fact. We may reasonably infer from the amended complaint that any set cookies had a marginal, even if *de minimis* and imperceptible, effect on the operation of those devices."[31] Based on this holding, the *PulsePoint* court found plaintiffs had alleged the requisite standing for their trespass on chattels claim.[32]

3. *Benefit of the bargain.*

The final argument often advanced by plaintiffs to demonstrate standing is often referred to as the "benefit of the bargain" theory. The basic gist of the argument is that plaintiffs entered into a contract with an online entity that included a privacy policy or data security provision. Despite paying the fee to enter into the contract, the defendant did not abide by its own promised privacy or security policy. Thus, plaintiff contends that she overpaid, and overpaid because she did not receive the full benefit of the bargain. Given the "overpayment" aspect of this argument, it is only alleged in cases where plaintiffs actually paid merchants or organizations for membership or other services of the website in question.

This argument, made both in the context of data breach and unwanted online tracking cases, has not been met with great success.[33] In rejecting the argument, courts often point to the fact that plaintiffs fail to allege how the ***15** data protection services they received were part of the contracted-promises for which the plaintiff actually paid.

In *Duqum v. Scottrade, Inc.*,[34] a data breach case, the plaintiff argued that he had standing based on the fact that he paid a brokerage and financial services fee to the defendant which in part included promised data security services.[35] The court rejected the argument, noting that the complaint was devoid of any facts showing that the services which plaintiff received were worth any less than what he bargained for, as plaintiff offered no allegations regarding what part of the fees paid for the brokerage services were understood by both parties to be allocated to data security services.[36]

The same issue precluded the court in *Austin-Spearman v. AARP*[37] from accepting plaintiff's benefit-of-the-bargain theory.[38] In that case, the plaintiff claimed that AARP allowed other Internet companies to track her web use, in contravention to its privacy policy, which was promised as part of her membership, for which she paid. The court found that the plaintiff received the benefit for which she paid, because the plaintiff could make no colorable argument that use of the AARP website was a primary, or even essential, benefit for which she paid.[39] The plaintiff received many benefits of her paid membership with AARP, such as the organization's advocacy for people over fifty years old. The court noted that

> conclusory statements regarding a plaintiff's own beliefs and expectations are not sufficient to support an alleged 'overpayment' injury; rather, a plaintiff must allege facts that demonstrate that the breached term was objectively essential to the contract at issue, such that the violation effectively robbed the plaintiff of her payment because what she received was not what the parties agreed she had purchased.[40]

Defendants raise the same argument in cases in which the plaintiff complains he or she did not receive the benefit of privacy or security services for which he or she paid when the same promised security and privacy measures are provided to non-paying users of the website in question. For instance, in *In re LinkedIn User Privacy Litigation*,[41] another data breach case, the court found that plaintiffs failed to allege that the plaintiffs actually provided consideration for the security services provided by LinkedIn.[42] ***16** The court's reasoning rested on the fact that LinkedIn promised its nonpaying members the same security services as it did to the subscribers of its premium service, for which plaintiffs had enrolled. Thus, the court found that, "when a member purchases a premium account upgrade, the bargain is not for a particular level of security, but actually for the advanced networking tools and capabilities to facilitate enhanced usage of LinkedIn's services."[43] The *AARP* court noted that the plaintiff's argument in that case suffered similar defects. As in *LinkedIn*, the court noted that the privacy agreement plaintiff claimed was part of the bargain she paid for applied to both paying AARP members as well as to non-member users of the website. This meant that "payment was not provided in consideration for the promises that AARP made in the Privacy Policy, or, put another way, the promises made in AARP's Privacy Policy were not a part of [plaintiff's] binding AARP membership contract."[44]

In the recent *Williams-Diggins v. Mercy Health* case, the court rejected the benefit-of-the-bargain theory based on a different issue--as long as an individual's private information remains private, he is not entitled to dictate the precise method the defendant uses to keep it that way.[45] In that case, the plaintiff brought suit against Mercy Health because, he alleged, it used software with known issues that potentially allowed unauthorized individuals to access patients' medical information. As with the above cases, the plaintiff argued that he suffered an economic injury because some portion of the payments he made were for data security measures that were not taken by the defendant. However, as the court pointed out, without evidence of an actual data breach, plaintiff "paid for healthcare services with the expectation that the personal information he provided or that was created through the care he received would not be disclosed to third parties who were not entitled to obtain it. That is what he received. Even if Defendant's approach to data security was clumsy, it was harmless, and that is fatal to Plaintiff's claim."[46]

The benefit-of-the-bargain cases reveal a provocative truth. Taking the rationale of such cases to its logical conclusion, as long as retailers, financial firms, or any other consumer-facing business can assert that their services are distinguished from security services,[47] plaintiffs face an uphill battle to ***17** successfully demonstrate harm through the benefit-of-the-bargain theory, unless the terms of use posted online somehow contained a provision that services are primarily for security services in such scenarios or online marketing touted the company's expertise in secure technology. However, as society continues to place more emphasis on consumers' privacy rights as to their data or content viewing histories, discussed further in Section IV, *infra*, courts (including in a recent case against a maker of Smart TVs) may become more accepting of the argument that privacy protections offered by a product or service is a factor that influences consumer purchasing decisions.[48]

B. Intangible Loss and Statutory Standing.

Aside from tangible harm allegations, plaintiffs have also sought to show an intangible loss sufficient to demonstrate standing for certain types of claims. These claims are often those specifically aimed at a person's violation of privacy, and include intrusion upon seclusion,[49] invasion of privacy,[50] the Federal Wiretap Act,[51] and the SCA.[52] In addition, contract claims, such as breach of contract and breach of the duty of good faith and fair dealing, only require a showing of nominal damages.[53]

Notably, the option for consumers to prove an injury-in-fact through a non-economic showing is greater in the context of specific, statutory provisions that grant standing. Standing under the Federal Wiretap Act and the SCA has been found pursuant to the doctrine of statutory standing, whereby "an Article III injury can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[54] Moreover, claims alleging violations of statutes or common law torts focused on protection ***18** of privacy have more success showing standing, as they specifically contemplate that the harm alleged will be the interference of a person's right to privacy.[55] Thus, when defendants in *Google* argued that the plaintiffs lacked standing "because they make insufficient allegations of pecuniary harm[,]" the court found that defendants' focus on economic injury was misplaced.[56] Instead, the court noted that a concrete, particularized, and actual injury "does not demand that a plaintiff suffer any particular type of harm to have standing .... Rather, the actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing."[57]

After *Spokeo v. Robins* was decided in 2016,[58] discussed in detail at the beginning of this Section III, *supra*, the Third Circuit was again presented with a similar case. The multi-district consolidated class action against Viacom, the owner of Nickelodeon, and Google, related to the two companies' tracking of children's web browsing and video-watching habits on Viacom's websites, despite Nick.com's promise that none of the children's personal information was collected or shared.[59] Specifically, plaintiffs alleged that Viacom placed its own first-party cookies on user's computers and Google, through its contract with Viacom, placed its own third-party cookies on user's computers, which allowed Google to track that user's browsing activity across any website on which the company placed ads.[60] The purpose of such tracking was to gather the browsing information and sell targeted advertisements based on browsing history. Plaintiffs brought claims alleging violations of the Federal Wiretap Act, the SCA, the CIPA, the Video Privacy Act, the New Jersey Computer Related Offenses Act, and for intrusion upon seclusion.[61]

Defendants asserted that Article III standing was lacking "because the disclosure of information about the plaintiffs' online activities does not qualify as an injury-in-fact." [62] The court rejected this argument, as it had in *Google*, noting again that defendants' focus on economic harm was misplaced. Moreover, the court examined the *Spokeo* decision and found that it did not impact its analysis. [63] Instead, the court found that, "[i]nsofar as ***19** *Spokeo* directs us to consider whether an alleged injury-in-fact 'has traditionally been regarded as providing a basis for a lawsuit,' *Google* noted that Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private." [64]

Courts in other jurisdictions have also shown a recent willingness to accept these sort of intangible losses to show standing. For instance, in *In re Vizio Consumer Privacy Litigation*, [65] plaintiffs sued the television manufacturer over its alleged use of "automatic content recognition software to collect and report consumers' content viewing history." [66] Plaintiffs alleged that, unbeknownst to them, Vizio collected this information and sold it to advertisers and media companies to use to deliver targeted advertisements to consumers. Moreover, plaintiffs argued that this information was not anonymous, providing studies that showed how the transmitted information is often sufficient to be linked to a specific individual. [67] The court found that this intangible harm was enough to show standing under the Video Privacy Protection Act, the Federal Wiretap Act, and the common law privacy torts alleged by plaintiffs. [68]

Defendants have also attempted to counter the argument that disclosure of plaintiffs' online browsing activities does not constitute an injury-in-fact when that information is anonymized. In *Cooper v. Slice Technologies, Inc.*, [69] plaintiffs contended that UnrollMe, a Slice Technologies subsidiary, collected plaintiffs' email addresses and sold the anonymized emails without plaintiffs' consent. [70] The court, relying on the Second Circuit's summary order affirming the decision in *PulsePoint*, found that selling anonymized information was enough to show standing for the Electronic Communications Privacy Act, the SCA, CIPA, unjust enrichment, and intrusion on privacy. [71]

Therefore, plaintiffs have at their disposal statutory rights of action, which present a greater risk to businesses because courts have generally found that a violation of the statutory right would establish standing. [72]

***20 IV. HOW MUCH ECONOMIC VALUE DOES CONSUMER DATA HAVE?**

In the cases described above, courts and litigants have exerted substantial efforts to demonstrate the monetary value that can be extracted from consumers' personal information. Interestingly, arguments concerning the financial-assets approach to gauging the value of data often arise in the context of standing debates. This is not necessarily surprising, since courts have concluded that if the basis of the injury is improper handling of personal information, a plaintiff must show that she "personally lost the opportunity to sell [her] information or that the value of [her] information was somehow diminished after it was collected." [73] Furthermore, in the breach context, a "growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory." [74]

However, what is the extent of such value? A national consumer reporting agency describes one potential metric for this data--the marketplace on the dark web for stolen data and personal information. Experian's reporting states that the ten most common pieces of information and price ranges include: up to $20 to $200 for online payment services login info or up to $1,000 or $2,000 for U.S. Passport information or $1,000 for medical records. [75] At the same time, however, one court found--citing to a 2011 study--that web browsing histories are worth $52 per year, users' contact information is worth $4.20 per year, and demographic information is worth $3.00 per year. [76]

Regardless of the true value, the existence of such studies and litigation findings demonstrates that as consumers become increasingly savvy with implications concerning the use of their PII, a greater risk to businesses may arise through enterprising plaintiffs filing suits, as they become motivated to extract personal benefit from such data.

V. WHAT DO CONSUMERS TRULY EXPECT BY WAY OF PRIVACY?

The existence of business risk is supported by the larger context of social science research about consumer preferences. Even with regular news of privacy breaches reaching the average consumer's consciousness, litigation ***21** and remediation through the courts seem to be of minimal interest for most consumers, though it appears that may be changing, with a greater emphasis on privacy concerns and a lesser emphasis on security concerns (breach). This appears to be the new trend, for many reasons.

First, studies have shown that while consumers do care about privacy, data breaches have been having relatively little long-term effect on consumers' perception of companies that have experienced data privacy breaches. Specifically, contrary to common expectations, consumers' trust of a company seems to derive from the consumer's *perception* of that company's data privacy protections rather than that company's actual track record of protecting data privacy.[77] As such, consumer perception of trustworthiness is more connected to how a company reacts to data breaches, rather than whether it has had data privacy breaches.[78] An example of this includes the fact that even after a company faces one or more large data breaches, unless consumers are reminded of a particular data breach, consumers continue to have a positive opinion of that company's trustworthiness over time.[79] Ultimately, data breaches or a history of data breaches do not appear to negatively affect consumer trust in the long-term.[80] In fact, studies have shown that the public's trust in Facebook, which has a long record of highly publicized data breaches, is actually higher than the public's trust in other companies with fewer data privacy issues.[81]

Second, and perhaps relatedly, it appears consumers are becoming desensitized to data breaches. In the past, consumers reported short-term drops in their perception of companies with data breaches. Recently, however, even the immediate effect on consumer perception appears to be *de minimis*. One study has hypothesized that this effect is due to "privacy fatigue," meaning that privacy breaches have become so commonplace that consumers no longer base their trust of a company on publicized privacy flaws, but rather on other considerations, such as the company's reaction to privacy breaches.[82] Surveys have also noted that current customers are less impacted by data breaches as opposed to potential customers due to the "*endowment effect*," or the idea that people place a higher value on things they own, or in this case, place more trust in companies that they are currently customers of.[83] Based on this data, it appears that safeguarding private data has grown to be of less concern to consumers as breaches have ***22** become more commonplace and are now seen by consumers as something to be expected.

Third, data breaches do not seem to drive consumer behavior. When a data breach occurs, consumers want information on the breach and how it is being mitigated, such as notifications to affected consumers explaining the risks or harms they are most likely to experience as a result of the breach.[84] However, despite consumer demands, studies show that when companies do give notifications and offer remedies, a large percentage of consumers take no action.[85] In a recent survey regarding post-breach consumer remedies, 63% of consumers feel that companies should offer identity theft protection, 58% feel that credit monitoring services should be required, and 67% feel that compensation through cash, product, or services is appropriate.[86] Put simply, after a breach, consumers appear to want some sort of remedy but do not act when receiving the remedy would require an affirmative action.

Moreover, consumers seem increasingly of the view that acting on or claiming the company-offered remedy is too inconvenient; perhaps the offered remedy does not make the consumer feel whole, or maybe the consumer is not informed of any offered remedy. The one commonality among all the reasons a consumer may not take a company up on its offered remedy is that these are company-imposed and company-regulated remedies. Ultimately, it is the companies that have been hit by data breaches that are deciding what to offer consumers to make them whole, and how to offer it to them. Up until recently, consumers have had little voice and little legal remedy to act against the companies through litigation and challenge these self-imposed remedies.

Consumers' failure to act in response to data breaches may also be a result of the relatively insignificant financial impact data breaches have on them as individuals. While a Federal Trade Commission study in 2003 estimated economic losses from data breaches to be in the billions of dollars, the impact of a breach on individual consumers is fairly low, with the average out-of-pocket cost only about $38.00.[87] This may explain why, despite demands for remediation and compensation, consumers often forego remedial actions and consumer interest in sweeping regulations or court involvement with data breaches is less than one might expect.

Fourth, consumers' increasing interest in Internet privacy rights outside of the breach context is apparent from the global proliferation of new laws targeted at protecting Internet privacy. Consumers are more concerned with control over the collection, use, and sharing of their data prior to a ***23** breach.[88] With recent legislative enactments in Europe through GDPR and California's Consumer Privacy Act of 2018, the conditions are ripe for a push from advocacy groups and plaintiff's attorneys to use consumers' focus on data privacy to push for more regulatory enforcement and litigation.

Against this backdrop, consumers' interest in data privacy is increasingly manifest in their desire for control over how their data is collected and used by companies. A vast majority of consumers believe an organization has an obligation to take reasonable steps to secure their personal information but do not make specific demands for protections or practices.[89] In general, consumers expect that these steps to secure their data should be sufficient so that, ultimately, the consumer is able to control how companies or organizations use their personal information.[90] Consumer sentiment regarding the need for firms that deal with personal data to take a proactive approach to safeguarding that data appears to be growing**.** A recent study has shown that a company just having access to personal data inflates a consumer's feeling of violation and reduces their overall trust.[91]

In fact, privacy is one of the most important, if not the most important, issues facing companies as studies have shown that consumers are more concerned with privacy than convenience, meaning consumers are concerned enough about privacy that they would rather connect to online businesses through mediums that are less able to track them despite any inconvenience that it may cause.[92] This evidence demonstrates consumer demand for data protection may be so great they are potentially unwilling to sacrifice it for a better user experience.

VI. CONCLUSION

Going forward, as public opinion evolves and increasingly concludes that merely possessing private data puts consumers at risk, consumers may demand concessions from institutions, retailers, and tech giants that possess personal data, whether or not they have been subjected to a large-scale data breach. To date, consumers have faced formidable barriers to relief in court by virtue of their inability to artfully allege all necessary facts to demonstrate standing. However, as consumers become more sophisticated regarding the monetary value of their data and knowledgeable about use cases for businesses selling or purchasing PII and viewing histories, consumers ***24** may become more well-versed in substantive technology so as to satisfy the current pleading standards. Furthermore, while new privacy legislative efforts are still under way, policy makers may view evolving trends as a justification for stronger consumer privacy protections. Legal challenges to damages are important for businesses, consumers, and lawmakers to understand as they grapple with the policy implications of new technology in consumer-facing businesses.

Footnotes

a1 *J.H. Jennifer Lee, a partner at Arent Fox, served as an Enforcement Attorney in the CFPB's Field Litigation Team for several years since the agency's inception. She now represents financial services clients in government investigations and complex litigation matters involving federal or state consumer financial statutes and implementing regulations.*

a2 *Kimberly B. Frumkin is an associate at Dorsey & Whitney. Her practice focuses on servicing the financial industry, from advising on regulatory and structuring considerations, to defending individuals and entities facing scrutiny by the regulating agencies.*

a3 *Susan Tran is an associate at Arent Fox. She represents financial services clients in a wide variety of settings involving both litigation and advising.*

a4 *Nicolás Sánchez-Mándery works in the banking and insurance fields, with a special focus on consumer finance rules.*

1 To be sure, current media reports concerning attacks by criminals or foreign governments have renewed public awareness of privacy and data concerns. Nevertheless, as early as several years before the 2016 presidential election, Facebook and other tech giants faced a panoply of privacy litigation matters asserting alleged violations relating to Internet cookies, Internet Load Objects, or comparable technology.

2 *See, e.g.*, LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532, at *1 (C.D. Cal. Apr. 28, 2011).

3 In June 2018 California adopted a privacy law that becomes effective January 2020, but appears to contain no provision to alter this situation. The law states: "Any consumer whose nonencrypted or nonredacted personal information ... is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater [;] (B) Injunctive or declaratory relief[;] (C) Any other relief the court deems proper." California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.150(a)(1) (West 2018). This provision, however, applies to security violations in the context of a data breach. Further, a bill analysis, conducted the day before the bill was signed into law, by the Assembly Committee on Privacy and Consumer Protection, indicates that the law authorizes a private right of action only for data breaches. *See* ASSEMBLY COMM. ON PRIVACY & CONSUMER PROT., INFORMATIONAL HEARING REPORT, AB 375, at 8-9 (June 17, 2018).

4 *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 131 (3d Cir. 2015).

5 Google was sued by the Department of Justice in the Northern District of California over its conduct, which it settled in 2012 for $22.5 million. Press Release, Federal Trade Commission, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser: Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented [https://perma.cc/Z3AX-5DQL]. In addition, thirty-eight state attorney generals also sued the company, which Google settled for $17 million in 2013. *See* Claire Cain Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. TIMES, Nov. 18, 2013, https://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html [https://perma.cc/9BWZ-VPR4].

6 *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d at 153.

7 *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 925 (N.D. Cal. 2015).

8 *Id.*

9 Order Granting Defendant's Motion to Dismiss, *In re* Facebook Tracking Litig., 263 F. Supp. 3d 836, 841 (N.D. Cal. 2017) (No. 5:12-md-02314-EJD).

10 *Id.* at 848-49.

11 *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992).

12 Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1548 (2016) (holding in a 6-2 decision addressing Fair Credit Reporting Act theories that actions based on an alleged technical, statutory violation, without a showing of "concrete" and "particularized" harm, did not satisfy the injury-in-fact requirement to establish standing). On remand, a three-judge panel of the Ninth Circuit held that dissemination of false information in consumer credit reports implicate harm to one's employment prospects that constitute a sufficiently "concrete" injury. *See* Robins v. Spokeo, Inc., 867 F.3d 1108, 1114-17 (9th Cir. 2017).

13 Bethman v. Faith, 462 S.W.3d 895, 901 (Mo. Ct. App. 2015) (quoting Schweich v. Nixon, 408 S.W.3d 769, 774 (Mo. 2013) (en banc) (citations and quotations omitted)).

14 *Spokeo*, 136 S.Ct. at 1548.

15 *Id.*

16 This is true in the majority of cases. However, in *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021, (N.D. Cal. 2012), the court found that the fact that plaintiffs' information was disclosed due to LinkedIn's policies was enough to establish standing for conversion and unjust enrichment claims.

17 The requirement of an economic loss under the CFAA is sometimes discussed as a standing issue, and other times framed as an element required to state a claim under the statute. *Compare In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 934 (N.D. Cal. 2015) (dismissing CFAA claim because of lack of standing) *with* Del Vecchio v. Amazon.com, Inc., No. C11-366RSL, 2012 WL 1997697, at *8-18 (W.D. Wash. June 1, 2012) (dismissing CFAA claim because no economic loss could be shown to make out a necessary element of the claim).

18 *See, e.g.*, Mount v. PulsePoint, Inc., No. 13-cv-6592, 2016 WL 5080131, at *9 (S.D.N.Y. Aug. 17, 2016), *aff 'd*, 684 Fed. App'x 32 (2d Cir. 2017); Order Granting Defendant's Motion to Dismiss, *In re* Facebook Tracking Litig., 263 F. Supp. 3d 836, 842 (N.D. Cal. 2017) (No. 5:12-md-02314-EJD).

19 Order Granting Defendant's Motion to Dismiss, *In re* Facebook Tracking Litig., 263 F. Supp. 3d 836, 843 (N.D. Cal. 2017) (No. 5:12-md-02314-EJD).

20 *See In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d at 934.

21 *See, e.g.*, LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532, at *11 n.1 (C.D. Cal. Apr. 28, 2011) (noting the court was declining to say it was categorically impossible for plaintiffs to allege some kind of property of privacy interest that was compromised by defendant's actions, but, by accepting defendant's framing of the issue, they failed to do so).

22 LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011).

23 *Id.* at *3.

24 *Id.* at *12.

25 *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d at 931-32.

26 *Id.*

27 Mount v. PulsePoint, Inc., No. 13-cv-6592, 2016 WL 5080131 (S.D.N.Y. Aug. 17, 2016), *aff 'd*, 684 Fed. App'x 32 (2d Cir. 2017).

28 *Id.* at *6.

29 *Id.* at *7.

30 LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 WL 1661532, at *13 (C.D. Cal. Apr. 28, 2011).

31 Mount v. PulsePoint, Inc., No. 13-cv-6592, 2016 WL 5080131, at *5 (S.D.N.Y. Aug. 17, 2016), *aff 'd*, 684 Fed. App'x 32 (2d Cir. 2017).

32 Although the court found that this *de minimis* injury was enough to show standing, it did not find that it was enough to state a claim for trespass to chattels. *Id.* at *29.

33 However, cases where a data breach has actually occurred have employed this argument with far more success than in those in which it has not. *See* Williams-Diggins v. Mercy Health, No. 16-cv-1938, 2018 WL 6387409, at *3 (Dec. 6, 2018 N.D. Ohio) (collecting cases).

34 Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001 (E.D. Mo. July 12, 2016).

35 *Id.* at *6.

36 *Id.* at *7.

37 Austin-Spearman v. AARP, 119 F. Supp. 3d 1 (D. D.C. 2015).

38 *Id.* at 11-12.

39 *Id.* at 12-13.

40 *Id.* at 13.

41 *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089 (N.D. Cal. 2013).

42 *Id.* at 1093.

43 *Id.*

44 *Austin-Spearman*, 119 F. Supp. 3d at 12.

45 Williams-Diggins, 2018 WL 6387409, at *2.

46 *Id.*

47 Plaintiffs have had more success when the service purchased is of the type where keeping information private is an important and significant aspect of the service, such as when the service is based around making secure payments. *See* Svenson v. Google Inc., No.13-CV-04080, 2015 WL 1503429, at *4 (N.D. Cal. Apr. 1, 2015) (finding that plaintiff showed damages and standing under the benefit of the bargain theory when she alleged "[t]he services Plaintiff and Class Members ultimately received in exchange for Defendants' cut of the App pur-chase price--payment processing, in which their information was unnecessarily divulged to an unaccountable third party--were worth quantifiably less than the services they agreed to accept, payment processing in which the data they communicated to Defendants would only be divulged under circumstances which never occurred").

48 *See, e.g.*, *In re* Vizio, Inc. Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1217 (C.D. Cal. 2017) (finding that plaintiffs' allegation that they "would not have purchased, or would have paid less for, their Vizio Smart TVs had Defendants not concealed their collection and disclosure of Plaintiffs' personal information" was enough to show standing under consumer protection claims).

49 *See, e.g.*, Mount v. PulsePoint, Inc., No. 13-cv-6592, 2016 WL 5080131, at *4 (S.D.N.Y. Aug. 17, 2016), *aff 'd*, 684 Fed. App'x 32 (2d Cir. 2017).

50 *See, e.g.*, Order Granting Defendant's Motion to Dismiss, *In re* Facebook Tracking Litig., 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (No. 5:12-md-02314-EJD).

51 *See id.* at 842 (citing 18 U.S.C. §§ 2510 et seq.).

52 *See id.* (citing 18 U.S.C. §§ 2701 et seq.).

53 *Id.* at 844.

54 *In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 932-34 (N.D. Cal. 2015).

55 *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125, 134 (3d Cir. 2015).

56 *Id.*

57 *Id.* (quoting Havens Realty Corp. v. Coleman, 455 U.S. 363, 373 (1982)).

58 Spokeo, 136 S.Ct. at 548 (holding under the Fair Credit Reporting Act, theories that actions based on an alleged technical, statutory violation, without a showing of "concrete" and "particularized" harm, did not satisfy the injury-in-fact requirement to establish standing).

59 *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 268-69 (3d Cir. 2016).

60 *Id.* at 269.

61 *Id.* at 271.

62 *Id.* at 272.

63 *Id.* at 274.

64 *Id.* (quoting Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1549 (2016)).

65 *In re* Vizio, Inc. Consumer Privacy Litig., 238 F. Supp. 3d 1204 (C.D. Cal. 2017).

66 *Id.* at 1212.

67 *Id.*

68 *Id.* at 1217.

69 Cooper v. Slice Technologies, Inc., No. 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018).

70 *Id.* at *1-2.

71 *Id.* at *1, 3.

72 As noted *supra* note 3, the California privacy law does not afford a private right of action unless there has been a data breach. Accordingly, the statutory provision that sets forth a private right of action would be inapposite for the purpose of allowing plaintiffs to establish standing based on the rationale of the cases discussed in this section above.

73 *See In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d 922, 931-32 (N.D. Cal. 2015).

74 *In re* Experian Data Breach Litig., No. SACV 15-1592 AG (DFMx), 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016); *see also In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016) ("[T]he consistent theme running through these decisions ... is that 'Loss of Value of PII' represents a cognizable form of economic injury.").

75 *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, Experian (Apr. 9, 2018), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [https://perma.cc/SW5H-XJQL].

76 *See In re* Facebook Internet Tracking Litig., 140 F. Supp. 3d at 928.

77 Sadia Afroz et al., *How Privacy Flaws Affect Consumer Perception*, *in* 2013 THIRD WORKSHOP ON SOCIO-TECHNICAL ASPECTS IN SECURITY AND TRUST 10-17 (2013).

78 *Id.*

79 *See id.*

80 *See id.*

81 *See id.*

82 *Id.*

83 *Id.*

84 PONEMON INST., THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT 1 (Apr. 2014).

85 *Id.* at 5.

86 *Id.*

87 *Id.* at 7.

88 *See id.*

89 PONEMON INST., THE IMPACT OF DATA BREACH ON REPUTATION 4 (May 2017).

90 *Id.* at 18.

91 *See* Kelly D. Martin, Abhishek Borah & Robert W. Palmatier, *Data Privacy: Effects on Customer and Firm Performance*, 81 J. MARKETING 36, 36-58 (2017).

92 *E.g.*, John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 617 (2018).

73 CONFLQR 6

End of Document