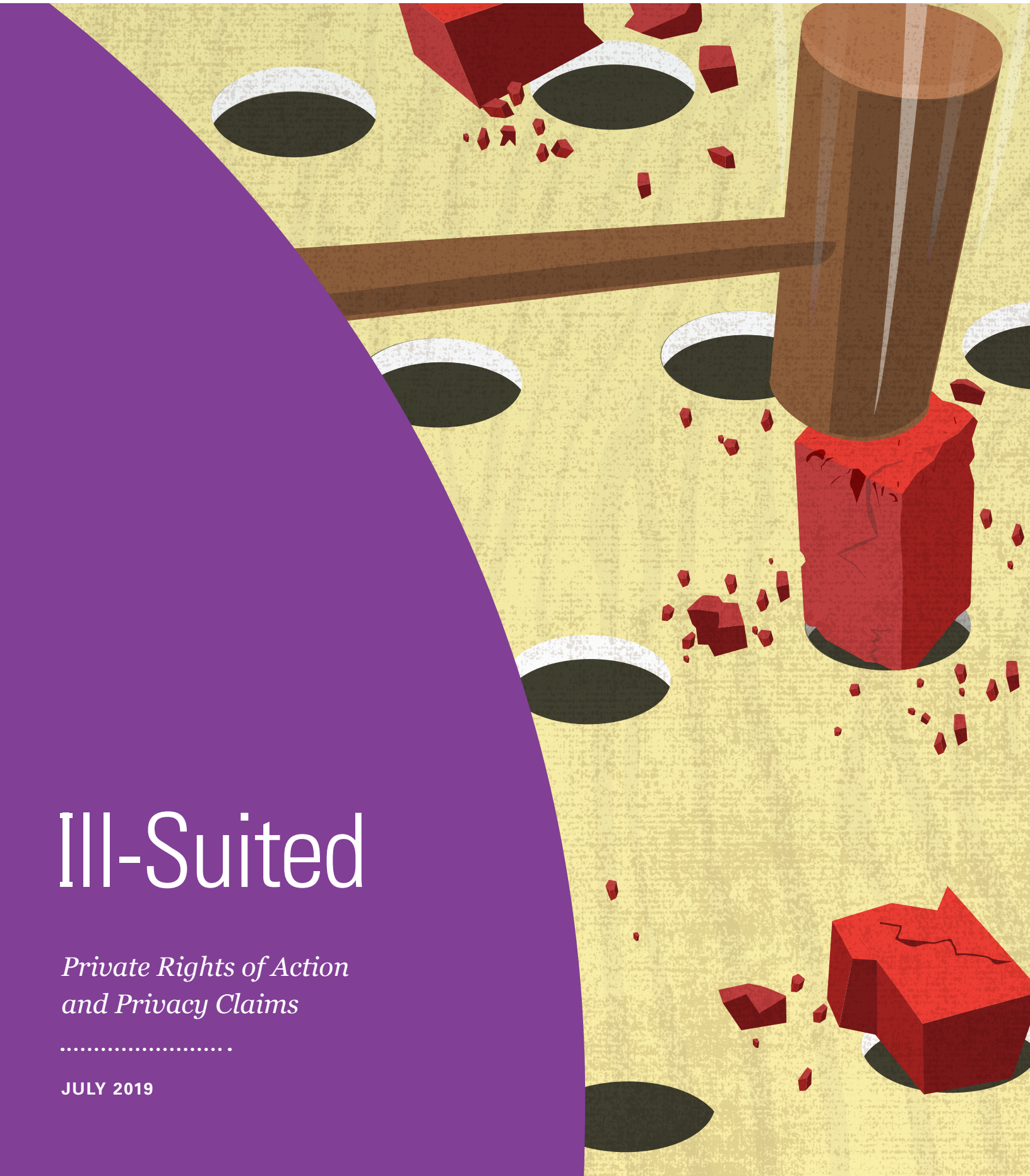
U.S. CHAMBER
Institute for Legal Reform



Ill-Suited

Private Rights of Action and Privacy Claims

JULY 2019

U.S. CHAMBER
Institute for Legal Reform

An Affiliate of the U.S. Chamber of Commerce

Table of Contents

Executive Summary 1

The Flood of Common Law, Tort-Based Privacy Actions 2

Statutory Private Rights of Action: Inefficient and Ineffective for Addressing Privacy Concerns 5

Detrimental Consequences of Privacy Private Rights of Action 14

Agency Enforcement 16

Conclusion 19

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

Mark Brennan, Adam Cooke, and Alicia Paller of Hogan Lovells US LLP

The author wishes to thank Joe Cavanaugh from Hogan Lovells for his assistance and contributions to this paper, along with Melissa Bianchi, Angela Krulc, and King Xia, also from Hogan Lovells.

Executive Summary

For years, the plaintiffs' bar has conjured multibillion-dollar class action lawsuits out of largely intangible privacy harms. This wave of litigation is increasingly driven by federal and state statutes that include private rights of action and allow for excessive statutory damages. Given the willingness of some courts to let cases proceed despite a lack of allegations or evidence of concrete harm, this litigation trend shows no sign of abating.

Unfortunately, this private litigation is especially problematic in the privacy context, as it undermines appropriate agency enforcement, clutters the courts, and chills innovation and nationwide service deployment. By contrast, privacy-related statutes that do not provide a private right of action, but rather delegate enforcement authority to agencies, often lead to far stronger outcomes that better balance penalties, deterrence, innovation, and consumer protection.

This paper examines troubling privacy class action litigation trends under common law, state statutes, and federal statutes, where plaintiffs' alleged harms are often intangible —or nonexistent—and where the wrongdoer is frequently unknown or unidentifiable. It focuses on suits brought under four laws to demonstrate why statutory private rights of action are inefficient and ineffective for addressing privacy concerns: the Telephone Consumer Protection Act (TCPA), the Fair Credit Reporting Act (FCRA), the Video Privacy Protection Act (VPPA), and the Illinois Biometric Information Privacy Act (BIPA). This paper then explores how plaintiffs resort to state privacy and consumer protection statutes to further sidestep congressional intent where private rights of action are not provided in federal statutes. Next, we highlight the overarching and statute-specific consequences that flow from privacy private rights of action, which harm both consumers and businesses. We then explain why privacy-related statutes that do not include private rights of action and instead delegate enforcement power to agencies are often far superior to private litigation.

The Flood of Common Law, Tort-Based Privacy Actions

Individuals have long brought common law tort suits to address specific, concrete harms caused by easily identifiable individuals or entities.

If a neighbor tramples your crops, he might be liable for trespass. If a thief takes a painting that you own, she might be liable for conversion. The injury for these torts was often obvious: my neighbor ruined my crops and I cannot sell them; the thief took my painting, which I no longer have. When it comes to privacy interests, however, "harms" are largely inchoate and intangible, and the wrongdoer(s) is or are often unknown or unidentifiable. We discuss below these harm and causation concerns in privacy class actions.

Intangible Harm

Although the plaintiffs' bar has frequently sought creative—and counterproductive—ways of bringing privacy claims under the guise of torts like trespass to chattels, negligence, and unjust enrichment, such claims are ill-suited to private enforcement. For example, plaintiffs bringing suit over location tracking or cookie tracking have often attempted to manufacture harms where none exist and have struggled to identify any cognizable injury.

They have, for instance, alleged that they suffered a loss of value of personally identifiable information (PII) as a result of defendants' conduct. Most courts have recognized, however, that loss of value of PII is insufficient to serve as Article III injury under the Supreme Court's guidance in *Spokeo v. Robins* or is insufficient injury under the causes of action presented.[1] And even if there were a cognizable harm, determining liability through case-by-case, district-by-district decisions fails to provide clear expectations for consumers or businesses.

"When it comes to privacy interests, however, 'harms' are largely inchoate and intangible, and the wrongdoer(s) is or are often unknown or unidentifiable."

> PulsePoint *and* LaCourt *demonstrate how intangible the 'harms' are in many privacy cases, and they are not alone in rejecting plaintiffs' 'harm' allegations.*

As an example, in *Mount v. PulsePoint, Inc.,* plaintiffs filed suit alleging that PulsePoint circumvented the privacy settings on their Safari web browsers to place third-party tracking cookies on their computers and mobile devices.[2] Plaintiffs asserted both common law tort claims (trespass to chattels and unjust enrichment) and claims under federal and state statutes (the Computer Fraud and Abuse Act and New York General Business Law Section 349).[3]

After hearing oral argument on PulsePoint's motion to dismiss, the court agreed with PulsePoint that plaintiffs failed to show any cognizable injury to support the claims asserted under New York common law, the Computer Fraud and Abuse Act, or the state's consumer protection statute.[4] The court held that plaintiffs had failed to allege the necessary harm to sustain their trespass to chattels claim because:

> There [were] no particularized allegations of diminished device performance. At most, plaintiffs [] plausibly alleged some unspecified increase in the use of device storage or processing capacity, without alleging that this uptick was significant or caused any discernible effect on the operation of the devices.[5]

The court also found that plaintiffs "failed to plead injury based on misappropriation of the value of their browsing information."[6] They did not allege that they were prevented from participating in programs that compensate individuals for web browsing data, or would receive less compensation from these programs, due to defendant's action.[7] The Second Circuit affirmed the dismissal, agreeing that plaintiffs failed to allege any actionable injury.[8] The collection of aggregated, anonymized web-browsing data did not constitute a cognizable invasion of privacy injury, and plaintiffs were not deprived of the ability to sell their browsing information and did not suffer diminished computer performance.[9]

Similarly, in *LaCourt v. Specific Media, Inc.,* plaintiffs brought claims under numerous statutes and for trespass to chattels and unjust enrichment.[10] Here too, the court rejected plaintiffs' threadbare allegations of harm. Plaintiffs failed to "identify a single individual who was foreclosed from entering into a 'value-for-value exchange' as a result of [defendant's] alleged conduct," and did not explain how they were allegedly "'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party."[11]

The court further noted that plaintiffs alleged no facts suggesting that they ascribed an economic value to their unspecified personal information.[12]

Plaintiffs' additional theory of harm—that their computers suffered from diminished performance capabilities—was also rejected as a "half-hearted" argument without factual support.[13] Thus, plaintiffs' claims were dismissed.[14]

PulsePoint and *LaCourt* demonstrate how intangible the "harms" are in many privacy cases, and they are not alone in rejecting plaintiffs' "harm" allegations.[15]

Suspect Causal Links

Even in cases where privacy interests are arguably more concrete, it is often impossible to fairly trace alleged harm to a particular party or defendant. Data breach litigation serves as a good example. Following a data breach, someone may be the victim of identity theft and incur tangible costs related to that identity theft event (e.g., monitoring service fees or overdraft fees). In the vast majority of cases, however, it is impossible to link that event to a particular data breach that a company suffered.

For example, in *Foster v. Essex Prop., Inc.,* plaintiffs alleged that unauthorized charges were made to their credit card following a data breach.[16] The court granted defendant's motion to dismiss both the statutory claims and tort claim because plaintiffs failed to demonstrate "a causal connection between the unauthorized charges on [a plaintiff's] credit card and the security breach of [defendant's] internal computer system."[17] Some courts focus in part on the period of time that passes between the initial data breach and any later-in-time identity theft in determining whether plaintiffs have pleaded a connection between the two occurrences.[18]

Even where months pass, however, some courts are nonetheless willing to infer causation at the pleading stage where plaintiffs allege that the breached information is the same as the information used to steal their identities.[19]

It is often even more difficult to link a data event to a particular defendant's act or omission that caused plaintiff's alleged harm, as defendants are victims of the same bad actors that harmed the plaintiffs. Companies are impacted both financially and reputationally following a data breach, and due to the prevalence of data breaches, it is increasingly difficult to link a particular incident to a particular individual's allegations of identity theft or other harm.[20] For example, an individual's information might have been breached within the same calendar year at her grocery store, her bank, and her doctor's office. And, most of the time, the true bad actors are not ultimately identified or held accountable.

"It is often even more difficult to link a data event to a particular defendant's act or omission that caused plaintiff's alleged harm, as defendants are victims of the same bad actors that harmed plaintiffs."

Statutory Private Rights of Action: Inefficient and Ineffective for Addressing Privacy Concerns

In addition to bringing creative common law claims, plaintiffs' lawyers have aggressively latched onto private rights of action under state and federal statutes to prosecute privacy-related claims.

These actions can be brought on behalf of a single individual but are frequently brought as nationwide class actions. The litigation often leads to a major payday for plaintiffs' attorneys, even where class members experienced no concrete harm. And, as explored in this section, even where class members may have suffered a concrete injury, the data indicates that they are unlikely to receive material compensatory or injunctive relief through private litigation.[21]

As discussed more fully below, rampant litigation under the federal TCPA[22] and FCRA[23] provides two examples of how private rights of action are ill-suited to address claims involving privacy interests. In addition, although class action plaintiffs have brought fewer suits under the federal VPPA[24] in recent years, that statute also remains a source of litigation for miscellaneous privacy grievances that do not fit within other existing statutory schemes. As another example, litigation under the Illinois BIPA[25] is particularly voluminous and problematic, forcing other states considering similar biometric laws to assess whether it truly makes sense to include a private right of action.

> *"[E]ven where class members may have suffered a concrete injury, the data indicates that they are unlikely to receive material compensatory or injunctive relief through private litigation."*

Where states have no privacy-specific statute, plaintiffs' lawyers often turn to general consumer protection or unfair business practices statutes, which often include private rights of action. These cases frequently proceed past the motion to dismiss stage and effectively pressure defendants to settle, despite minimal allegations of harm (although plaintiffs sometimes struggle to achieve class certification).

Telephone Consumer Protection Act

Because of the TCPA, millions of dollars have been diverted to the plaintiffs' bar for calls that were never answered, and for calls and text messages that people want to receive. The TCPA was enacted in 1991—"[i]n what was thought to be telemarketing's heyday"[26]—to restrict calls that relied on random or sequential numbers, using an "autodialer," as well as calls made with a prerecorded or artificial voice. Today, the TCPA is used to squeeze money out of legitimate American companies that call or text consumers, even if those calls go unanswered, or if the messages were requested by a prior owner of a reassigned telephone number.

For example, consider a situation where an individual wants to receive text messages regarding upcoming doctor appointments, package deliveries, ride share services, or grocery drop-offs. Next, that person receives a new phone number through her employer, and the old phone number is recycled. Once the phone number is reassigned, the doctor's office, package delivery service, ride share, or grocery service texts the new holder of the recycled phone number, without knowing that the phone number was reassigned. These companies find themselves unexpectedly defending TCPA litigation, instead of the TCPA being used to prevent abusive fraud and scam robocalls.[27]

> *"[C]ompanies find themselves unexpectedly defending TCPA litigation, instead of the TCPA being used to prevent abusive fraud and scam robocalls."*

There is no statutory cap on damages under the TCPA, and courts have unfortunately nearly uniformly held that unsolicited contact in a TCPA case can satisfy the constitutional injury-in-fact requirement (i.e., a plaintiff has suffered or imminently will suffer a concrete and particularized harm, whether economic or not). Combined, these factors contribute to the high frequency of TCPA case filings. Suddenly, faced with enterprise viability-threatening TCPA litigation, throngs of companies have been on the hook for monetary penalties that far outpace Congress' original intent for the TCPA.[28]

For example, the Second Circuit recently held in *Melito v. Experian Mktg. Solutions, Inc.,* that TCPA plaintiffs who receive an unsolicited text message meet the Article III injury-in-fact requirement, even without alleging any other harm, because such

> *"Under these conditions, court dockets are unduly cluttered, companies are forced to expend resources on baseless litigation, and plaintiffs' lawyers carry on enriched, emboldened, and ready to press repeat."*

texts are a "nuisance and privacy invasion."[29] This holding aligns with certain prior TCPA standing decisions in the Third and Ninth Circuits.[30]

It is remarkably easy for plaintiffs to file complaints under the TCPA and force companies to spend significant resources litigating or settling these cases, even though mere technical violations may be alleged. Many TCPA suits also allege that consent was obtained, but not according to the specific requirements of the statute or the Federal Communications Commission's (FCC) TCPA implementing rules. And, for fax advertisements, even providing a substantially compliant opt-out notice can still lead to class action exposure.

Making things worse, the FCC issued a misguided Declaratory Ruling and Order in 2015 that sought to provide clarification regarding a number of TCPA issues.[31] Following the "clarification" (which the D.C. Circuit later struck down in key respects), TCPA litigation increased dramatically.[32,33] In the 17-month period before the FCC issued the Order, 2,127 TCPA suits were filed; in the 17-month period following the FCC Order, 3,121 suits were filed.[34]

More recently, while overall TCPA litigation has declined slightly, the percentage of TCPA suits filed as class actions has grown startlingly high. In March 2019, 120 of 287 (41.8 percent) TCPA suits filed were putative class actions.[35] In April 2019, 98 of 294 (33.6 percent) TCPA suits filed were putative class actions.[36] And, in May 2019, 89 of 348 (25.6 percent) TCPA suits filed were putative class actions.[37] This significant exposure tends to lead companies to settle rather than continue to litigate, even though class certification has proved more challenging for TCPA plaintiffs.

Despite the theoretical comfort that some consumers may take in being able to sue where a private right of action is available, in TCPA settlements—as with many class action settlements—a few consumers walk away with at most trivial monetary compensation or vouchers, and most consumers are bound by the class settlement but recover no compensation at all.

For example, most TCPA settlement agreements establish a fixed-size settlement fund which pays out to claiming members pro rata. Historical claim rates in TCPA suits sit between four percent and eight percent.[38] Indeed, even sub-two percent claim rates can be approved.[39] Class members who claim a piece of the settlement fund walk away with a token amount, and the approximately 92 to 96 percent of class members who do not

submit a claim walk away with nothing.[40] Other times, claimants are offered vouchers for defendants' products or services.[41] Meanwhile, class counsel frequently seeks millions of dollars in attorney's fees in the amount of one third of the settlement,[42] and courts routinely approve final settlements allotting 25 to 30 percent of the settlement fund to go to class counsel.[43] Under these conditions, court dockets are unduly cluttered, companies are forced to expend resources on baseless litigation, and plaintiffs' lawyers carry on enriched, emboldened, and ready to press repeat.[44]

Fair Credit Reporting Act

FCRA class action lawsuits, often based on mere technical violations, continue to snowball. Congress enacted FCRA to "promote[] the accuracy, fairness, and privacy of information in the files of consumer reporting agencies."[45] The Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) enforce FCRA, in addition to there being private enforcement under the Act's private right of action.[46]

Today, two types of litigation are common under FCRA: suits alleging inaccurate information provided by consumer reporting agencies; and suits alleging that employers failed to abide by the Act's disclosure and notice requirements. Reports in 2018 confirmed that FCRA litigation increased by four percent from 2017.[47] These large sum suits often involve multiple plaintiffs or class action allegations, and increasingly are filed by employees and job applicants alleging deficiencies in defendants' disclosures.[48]

Many FCRA suits have made headlines in recent years, including those stemming from plaintiffs' attempts to capitalize on technical violations. In *Spokeo, Inc. v. Robins,* the plaintiff alleged that a data broker had violated procedural requirements under FCRA by publishing incorrect information about him online.[49] The Supreme Court held that "not all inaccuracies cause harm or present any material risk of harm." Injury in fact must be "concrete," and simply alleging a statutory violation does not always establish a concrete injury.[50]

The Court identified two key factors to determine whether "intangible harm" is a concrete injury: whether intangible harm "has a close relationship to a harm that has traditionally been regarded as providing a

> *"In* Spokeo, *... [t]he Supreme Court held that 'not all inaccuracies cause harm or present any material risk of harm.' Injury in fact must be 'concrete,' and simply alleging a statutory violation does not always establish a concrete injury."*

basis for a lawsuit in English or American courts," and whether Congress intended to elevate an intangible harm to the status of concrete injury.[51]

Although the Supreme Court drew a line between mere statutory violations and actionable harm, plaintiffs continue to push the limits where little, if any, harm exists. Several courts (including the Ninth Circuit when it considered *Spokeo* again on remand) have found an alleged dissemination of inaccurate information, in violation of FCRA, sufficient to establish injury in fact.[52] And, numerous FCRA cases have resulted in multimillion-dollar settlements, in part because defendants face uncapped damages.[53] As with TCPA suits, while defendants part with large sums to settle FCRA cases, a relatively small amount ends up in consumers' (class members') pockets.[54]

Video Privacy Protection Act

Today, claims lodged under the VPPA are routinely dismissed as falling beyond the scope of what the statute was meant to protect. In 1988, Congress passed the VPPA in response to a newspaper's publication of the video rental history of then-Supreme Court nominee Robert Bork.[55] The statute was meant to protect the privacy of video rental or purchase histories, providing consumers with a private right of action to sue video tape service providers for knowingly disclosing personally identifiable information. How and where people rent, purchase, and watch video has significantly changed since the VPPA was passed, yet plaintiffs' attorneys have reinvigorated the statute to go after companies for alleged wrongful "disclosures" of information.

Some courts have also interpreted Article III standing liberally with respect to the VPPA, which creates additional liability exposure and litigation costs.[56] The low standing hurdle benefits class action plaintiffs and acts as leverage against defendant companies.

For example, in *Yershov v. Gannet Satellite Info. Network, Inc.,* the First Circuit affirmed the district court's holding that a device identifier, video viewing data, and user geolocation information from the *USA Today* mobile application was "personally identifiable information" and held—contrary to the lower court's decision—that the plaintiff was a "consumer" under the Act.[57] This ruling extended the VPPA to a new platform (i.e., a mobile app) and further stretched the definitions of "personally identifiable" and "video tape service provider."[58]

More recently, in *Eichenberger v. ESPN,* the Ninth Circuit affirmed the district court's dismissal on the basis that the information at issue was not "personally identifiable information" under the VPPA.[59] Eichenberger sued over the alleged disclosure of his device serial number and the names of the videos that he viewed.[60]

The Ninth Circuit held that because that information would not "readily permit an ordinary person to identify a specific individual's video-watching behavior," it was not protected by the VPPA, which protects only "personally identifiable information."[61]

The Ninth Circuit suggested that the 1988 Congress did not intend for the VPPA to

cover circumstances like those alleged, which were "so different from the ones that motivated its passage."[62] While the narrowing *Eichenberger* decision might lead courts to be more skeptical of plaintiffs' mismatched claims under the VPPA, the private right of action continues to burden defendants whose activities ultimately might not be covered by the Act.

The Illinois Biometric Information Privacy Act and Other States' Regulation of Biometric Privacy

Multiple states have passed or are considering legislation to regulate the collection, use, and destruction of biometric information. Many of these statutes do not include a private right of action, and instead they appropriately delegate enforcement authority to state attorneys general or consumer protection divisions. Illinois is currently the outlier as the only state that provides a private right of action for biometric privacy.

BIPA

Plaintiffs' firms are now filing dozens of boilerplate complaints every month under the Illinois BIPA. The state law: (1) regulates the retention and destruction of biometric information; (2) prohibits the collection, retention, or disclosure of biometric information without providing certain information to data subjects in writing and receiving written consent; (3) prohibits selling, leasing, trading, or otherwise profiting from biometric information; and (4) restricts the disclosure of biometric information.[63] It is the only state biometric privacy statute that provides a private right of action.[64]

Moreover, BIPA and the Illinois Supreme Court have provided strong incentives for the plaintiffs' bar to file suits. The Act allows for recovery of $1,000 for each unintentional violation of the statute and $5,000 for each intentional violation of the statute,[65] and the Illinois Supreme Court confirmed that plaintiffs need not suffer actual harm to litigate under the Act.[66] Within this environment, Illinois consumers' choices are reduced, as companies understandably must assess what technologies or features to make available within the state.[67]

Although BIPA was enacted in 2008, it did not see much action in the courts until nearly a decade later. The first class-wide settlement under BIPA—for $1.5 million—was approved in 2016.[68] Courts saw a significant uptick in BIPA litigation in the years that followed.

Not only has there been a recent wave of litigation under BIPA, with more than 200 suits filed over the past two years alone, but the filing rate has skyrocketed since the January 2019 Illinois Supreme Court decision in *Rosenbach v. Six Flags Entertainment Corp.*[69] This decision emboldened the plaintiffs' bar, holding that no actual harm is required to be a "person aggrieved" under BIPA:

> [W]hen a private entity fails to comply with one of [BIPA's] requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach ... [S]uch a person would clearly be 'aggrieved' within the meaning of ... the

> Act and entitled to seek recovery ... . No additional consequences need be pleaded or proved.[70]

In the six months since the Illinois Supreme Court issued the *Rosenbach* decision, more than 100 new suits have been filed.

With many of these cases pending, courts have not yet explored BIPA's "per violation" scheme, and some are concerned that every fingerprint scan, for example, could count. Damages are not capped,[71] and liability could be astronomical, especially for companies that use biometric scans to record timekeeping information, such as who clocks in when they arrive in the morning, who clocks out for breaks and lunch, and who clocks out again at the end of the day. Each scan could potentially add up to four or more violations per timekeeper, per day.

"Liability could be astronomical, especially for companies that use biometric scans to record timekeeping information, such as who clocks in when they arrive in the morning, who clocks out for breaks and lunch, and who clocks out again at the end of the day."

In response to the unbounded proliferation of biometric privacy suits post-*Rosenbach*, the Illinois legislature proposed in March 2019 an amendment that would remove the private right of action. Instead, enforcement would be delegated to the Illinois Department of Labor and the state attorney general. The bill did not pass within the short timeframe provided and was therefore sent back to the Committee on Assignments. It remains to be seen whether this bill will be resubmitted for consideration.

In the meantime, parties continue to debate whether and when cognizable harm exists under BIPA. In June 2019, Facebook urged the Ninth Circuit to de-certify a BIPA class. Facebook argued that no invasion of privacy exists prior to misuse of data by defendants, and that class members agreed to Facebook's terms of service before using the facial mapping and recognition tool in question.[72] Facebook's counsel argued that in light of users' option to opt-out: "You can't walk into federal court and say, 'I really like this feature, I know how to opt out, I'm choosing to keep the feature on, but give me a thousand dollars.'"[73] While it remains to be seen how the Ninth Circuit will rule, these arguments highlight the tension between statutory protections and real-life examples of how users interact with, and benefit from, technology.

REGULATION OF BIOMETRIC INFORMATION BEYOND ILLINOIS

States beyond Illinois are largely grappling with decisions about the proper mechanism for enforcing legislation regarding biometric information. Relatedly, some states have included biometric data in existing or pending statutory definitions of "personal

information," including Massachusetts, Connecticut, Rhode Island, and California.[74] Some laws broadly protect biometric information, while other laws protect only biometric information used for authentication purposes.[75] Most of these statutes, however, do not include private rights of action. The California Consumer Privacy Act of 2018 (CCPA), for example, defines personal information to include biometric information,[76] but provides a private right of action only following certain data breaches.

Texas and Washington have existing biometric privacy legislation based on the Illinois BIPA, and although the statutes' requirements and restrictions vary,[77] both provide for enforcement by state attorneys general instead of a private right.[78] A host of other states have recently considered or are currently considering laws, similar to the Illinois BIPA, that would grant a private right of action, including Alaska, Florida, Michigan, New Hampshire, and New York.[79]

Other states have considered or are considering legislation more similar to Texas' and Washington's biometric privacy acts—which do not grant a private right of action—including Arizona and Montana (where the attorneys general would be responsible for enforcement), and Delaware (where the Delaware Protection Unit would be responsible for enforcement).[80] Whether and how states beyond Illinois regulate the collection, use, retention, and destruction of biometric information—and whether they provide a private right of action for violations of biometric privacy laws—will likely influence the extent to which companies offer innovative technology to employers and consumers across the country on equal footing, as we have seen occur in Illinois.

"Whether and how states beyond Illinois regulate the collection, use, retention, and destruction of biometric information—and whether they provide a private right of action for violations of biometric privacy laws—will likely influence the extent to which companies offer innovative technology across the country on equal footing..."

OTHER STATE PRIVACY AND CONSUMER PROTECTION STATUTES

Some state privacy and consumer protection statutes may give plaintiffs room to sidestep congressional intent where analogous federal statutes provide no private right of action. California's private right of action under its Unfair Competition Law (UCL), for example, has allowed plaintiffs to assert privacy claims based on or inspired by federal statutes that expressly have no private right of action, such as the Health Insurance Portability and Accountability Act (HIPAA).[81] These end-runs around congressional intent are

“The failure of a broader CCPA private right of action to advance in the California Senate is indicative of the drastic consequences that flow from expansive private rights of action...”

detrimental to the careful balance that must be struck between patient privacy, the swift and efficient provision of healthcare, and effective, uniform enforcement.

For example, in *Gardner v. Health Net, Inc.,* plaintiffs sued under the California UCL after an unencrypted portable disk drive containing social security numbers and bank account information was stolen from the defendant's office.[82] The UCL claim was predicated on numerous acts, including HIPAA violations.[83] The court held that "[a] HIPAA violation may constitute an unlawful business practice for the purpose of establishing liability under the UCL," although plaintiffs failed to set forth facts to support their allegations that defendant violated HIPAA.[84]

The CCPA may soon provide new opportunities for consumer litigation within the privacy sphere.[85] With many of its provisions set to become effective on January 1, 2020, the CCPA provides a private right of action to bring suits where nonencrypted or nonredacted personal information is subject to unauthorized access, exfiltration, theft, or disclosure as a result of a business' violation of its duty to implement and maintain reasonable security procedures.[86] Under the CCPA, consumers may seek actual or statutory damages between $100 and $750 per incident.[87] Consumers also may seek injunctive or declaratory relief, or other relief as deemed appropriate by a court.[88]

In May 2019, the California Senate declined to advance a bill that would have expanded the private right of action under the CCPA, thus avoiding the potential for more unfettered litigation.[89] While consumers will retain the limited right to bring litigation regarding certain alleged breaches, only the California Attorney General's office may enforce other provisions of the CCPA, seeking up to $7,500 per intentional violation, and $2,500 per unintentional violation.[90] The failure of a broader CCPA private right of action to advance in the California Senate is indicative of the drastic consequences that flow from expansive private rights of action, and will hopefully encourage other legislators to proceed with caution as they consider enforcement schemes to address similar privacy concerns.

Detrimental Consequences of Privacy Private Rights of Action

A stream of detrimental consequences flow from private rights of action as a mechanism to address privacy harms.

Some notable examples include:

FIRST
Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.[91]

SECOND
They can also lead to a series of inconsistent and dramatically varied, district-by-district court rulings.[92] Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.[93]

THIRD
Combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, private rights of action are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionally benefit plaintiffs' lawyers rather than individuals whose privacy interests may have been infringed.[94]

FOURTH
They also hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.[95]

"Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections."

The private rights of action available under the federal and state statutes discussed above raise additional issues and challenges:

FIRST
Rampant TCPA litigation drains judicial resources and leads to disparate treatment of what is actionable under the statute's broad or undefined terms. As courts grapple with whether and when to hold companies liable for violating the TCPA, the threat of liability impedes the ability of businesses across industries to best serve customers and patients in the smartphone era.

SECOND
FCRA is a breeding ground for long-lasting litigation where procedural violations exist without concrete harm. Minor technical violations lead to disproportionate risk as repeat players (both plaintiffs and plaintiffs' counsel) are quick to file boilerplate FCRA complaints.[96]

THIRD
The VPPA has become known as the statute that encourages plaintiffs' attorneys to try to fit a square peg in a round hole. These suits largely clutter the courts regarding scenarios that do not fit within the protections that the VPPA provides. It is yet another example of the inefficiencies that flow from abused and overused private rights of actions in the privacy sphere.

FOURTH
BIPA is crippling both technological innovation and business growth in Illinois. BIPA has been criticized as making Illinois "inhospitable to tech firms and businesses in general," affecting tech- and non-tech-based employers and costing the state both jobs and revenue.[97]

These issues can be largely if not entirely avoided by shifting enforcement power from plaintiffs (and plaintiffs' counsel) to experts within government agencies and offices. Congress has created numerous federal statutes that are enforced solely by government agencies. In the privacy sphere in particular, agency enforcement benefits consumers and patients, the entities that provide services to them, and the public at large.

Agency Enforcement

As discussed in more detail below, in the privacy context, agency enforcement is far superior to private litigation and strikes a better balance between protection, penalties, deterrence, and progress.

Agency enforcement is typically led by experts who are familiar with standards and best practices, who are intimately aware of the workings of relevant industries, and who have a thorough understanding of the regulations with which they seek compliance. Unlike litigation trumped up by the plaintiffs' bar to reach a quick payday, enforcement actions at their core are meant to identify and remedy noncompliance that raises concerns for consumer and patient privacy and promote fair competition within industries.

Agency-made decisions are also subject to oversight by administrative law judges, Congress, and/or the President. Moreover, Congress and the President are subject to voter action. These checks and balances help further develop consistent and appropriate policies and penalties.

Examples of federal legislation that provide no private cause of action for privacy violations and that are enforced by agencies include: HIPAA,[98] the Children's Online Privacy Protection Act (COPPA),[99] the Federal Educational Rights and Privacy Act (FERPA),[100] and the Genetic Information Nondiscrimination Act (GINA).[101] This Section focuses on HIPAA and COPPA as examples of impactful agency enforcement of diverse privacy interests.

HIPAA

HIPAA includes the Privacy and Security Rules, which are enforced by the Office for

"Unlike litigation trumped up by the plaintiffs' bar to reach a quick payday, enforcement actions at their core are meant to identify and remedy noncompliance that raises concerns for consumer and patient privacy and promote fair competition within industries."

Civil Rights (OCR), within the U.S. Department of Health and Human Services.[102] There is no private right of action under HIPAA, although individuals can file a complaint with OCR to initiate an investigation.[103] OCR enforces HIPAA not only by investigating complaints, but also by conducting compliance reviews to evaluate whether entities subject to HIPAA are in compliance, by educating third parties to increase compliance with the Act, and by referring possible criminal violations to the Department of Justice.[104]

OCR investigations can lead to any of a variety of outcomes, fostering resolution that tracks the severity and duration of HIPAA violations. For example, OCR can determine that a violation did not occur, or that the entity is not subject to HIPAA. Or, OCR can determine that a violation occurred and can obtain voluntary compliance from the covered entity and reach agreement regarding a corrective action plan.[105] OCR can also issue formal findings of a violation and impose civil monetary penalties.[106] These civil penalties are carefully prescribed, based on increasing willfulness, as follows:

> *"There are numerous benefits to HIPAA's agency enforcement scheme as compared to reliance on a private right of action."*

- Tier 1: $100-$50,000 per unknowing violation, capped at $25,000 per year the issue persisted (with a six-year statute of limitations);
- Tier 2: $1,000-$50,000 per reasonable cause violation, capped at $100,000 per year the issue persisted (with a six-year statute of limitations);
- Tier 3: $10,000-$50,000 per violation by willful neglect but timely corrected, capped at $250,000 per year the issue persisted (with a six-year statute of limitations);
- Tier 4: $50,000 per violation by willful neglect and not timely corrected, capped at $1.5 million per year the issue persisted (with a six-year statute of limitations).[107]

There are numerous benefits to HIPAA's agency enforcement scheme as compared to reliance on a private right of action. For example, patients who may be dissatisfied when interacting with healthcare institutions regarding traumatic, expensive, and even life-threatening medical conditions may be more eager to instigate litigation regarding private information than other groups, regardless of whether HIPAA was violated. HIPAA instead tasks experienced regulators with investigating violations and determining the appropriate sanctions.[108]

OCR works with covered entities to change their behavior and achieve compliance with the regulations, and uses monetary penalties to help address and deter noncompliance. Their process is viewed as structured, thorough, and expansive enough to correct violations while including prescribed limitations so as not to cripple

the industry with penalties and uncertainty. While staunch advocates for privacy-related private rights of action caution that agencies have limited resources to enforce statutory protections, OCR demonstrates how extensive agency investigations and enforcement can be: as of June 16, 2019, there were 485 breaches reported to OCR within the prior 24 months, all of which were under investigation by OCR.[109]

COPPA

The Children's Online Privacy Protection Act, enacted in 2000 and updated in 2013, provides only for enforcement by the FTC and state attorneys general. COPPA "requires companies collecting personal information from children under the age of 13 to post clear privacy policies and to notify parents and get their verifiable consent before collecting, using, or sharing personal information about a child."[110] The FTC has pursued more than 30 COPPA enforcement actions, leading to a variety of fact-specific penalties and outcomes.[111]

For example, in February 2019, the FTC entered a COPPA-related settlement with Musical.ly (now TikTok) for failure to seek parental consent to collect children's information. The company paid a $5.7 million fine, which marked the largest civil COPPA penalty received by the FTC.[112] This large fine reflected Musical.ly's knowledge that children were using the app and providing protected personal information, yet failure to seek the required parental consent in accordance with COPPA.[113] In addition to FTC enforcement, state attorneys general are also actively protecting rights guaranteed by COPPA.

The FTC also issued a warning letter to the operator of three dating apps, since the apps were collecting children users' birthdates, email addresses, photographs, and geolocation data.[114] The FTC imposed no fine, but advised the operator to take immediate action to comply with COPPA.[115] The agency also issued a consumer alert to warn parents about the dating apps, and the apps have been removed from major app stores.[116]

Conclusion

Although privacy law presents many complex questions about what to protect, why, how, and to what degree, the question of how best to enforce privacy rights has become increasingly clear.

Agency enforcement is far more beneficial to consumers and the organizations that serve them than unpredictable and excessive attorney-driven private litigation. Federal and state privacy statutes that provide private rights of action—like the TCPA, FCRA, VPPA, and Illinois BIPA—exemplify the pitfalls associated with allowing plaintiffs' lawyers to set policy nationwide by way of inconsistent judicial rulings. By contrast, privacy statutes that are enforced by government agencies provide a robust process through which noncompliance with protected privacy interests can be identified, remedied, and monitored while promoting consistency, fairness, and innovation.

Endnotes

1 *Spokeo v. Robins,* 136 S. Ct. 1540 (2016).

2 No. 13-CIV-6592(NRB), 2016 WL 5080131 (S.D.N.Y. Aug. 17, 2016), *aff'd,* 684 F. App'x 32 (2d Cir. 2017), as amended (May 3, 2017).

3 *Id.*

4 *Id.*

5 *Id.* at *9.

6 *Id.* at *13.

7 *Id.* at *6.

8 *Mount v. PulsePoint, Inc.,* 684 F. App'x 32 (2d. Cir. 2017).

9 *Id.* at *35-36.

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

11 *Id.* at *5.

12 *Id.*

13 *Id.*

14 *Id.*

15 *See e.g., In re Facebook Internet Tracking Litig.,* No. 5:12-md-02314-EJD, 2015 WL 6438744, at *5-6 (N.D. Cal. Oct. 23, 2015) (finding no Article III injury where plaintiff failed to show lost opportunity to sell information or that its value was diminished by defendant's actions); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *4 (N.D. Cal. Mar. 26, 2013) (holding that plaintiff failed to allege harm to support suit under numerous statutes and common law theories, including trespass to personal property and conversion, where plaintiff did not allege that Pandora attempted to sell his PII or would do so in the future); *Low v. LinkedIn Corp.,* No. 11-CV-01468-LHK, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011) (dismissing plaintiff's suit under various state statutes and common law theories, including conversion and unjust enrichment, where plaintiff's allegations that his PII had an "independent economic value" and that he was "unjustly compensated" when LinkedIn transferred his PII were "too abstract and hypothetical").

16 *Foster v. Essex Prop., Inc.,* No. 5:14-CV-05531-EJD, 2017 WL 264390, at *2 (N.D. Cal. Jan. 20, 2017).

17 *Id.* at *3.

18 *See, e.g., Resnick v. AvMed, Inc.,* 693 F.3d 1317, 1327 (11th Cir. 2012) (holding that a "mere temporal connection is not sufficient" but expressing increased skepticism due to the passage of months—instead of weeks—between the breach and the identity theft).

19 *Id.* (overturning lower court's decision where plaintiffs' pleadings "allege[d] a nexus between the two events that include[d] more than a coincidence of time and sequence").

20 *What is a Data Breach? Ultimate Guide to Cyber Security Breaches in 2019*, DNSSTUFF, (May 31, 2019), https://www.dnsstuff.com/data-breach-101 ("[R]esearch ... indicates that the average cost of a data breach in 2018 rose by 6.4% compared with the previous year to a total of $3.86 million ... [and] the average cost of each stolen file also increased to $148."); *The Impact of Data Breaches on Reputation & Share Value,* PONEMON INSTITUTE, (May 2017), https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf (113 companies experienced an average stock price decline of five percent after announcement of a data breach, and 65 percent of consumers surveyed said they lost trust in a company following a breach, thereby demonstrating both the financial and reputational harms companies experience).

21 *See, e.g., Mahoney v. TT of Pine Ridge, Inc.,* 2017 U.S. Dist. LEXIS 217470 (S.D. Fla. 2017) (granting TCPA settlement for $15 voucher or $4 cash); Letter from Monica S. Desai (Counsel to Wells Fargo) to Marlene H. Dortch (Secretary, FCC) (Jan. 26, 2015), https://ecfsapi.fcc.gov/file/60001016697.pdf.

22 42 U.S.C. § 227.

23 15 U.S.C. § 1681.

24 18 U.S.C. § 2710.

25 740 Ill. Comp. Stat. 14/1 *et seq.*

26 *Duguid v. Facebook, Inc.,* No. 17-15320, 2019 WL 2454853, at *1 (9th Cir. June 13, 2019).

27 Stuart L. Pardau, *Good Intentions and the Road to Regulatory Hell: How the TCPA went from Consumer Protection Statute to Litigation Nightmare*, 2018 U. Ill. Tech. & Pol'y 313 (2018).

28 *Internet Association Asks Court to Vacate Sweeping TCPA Rules*, Internet Ass'n (Dec. 2, 2015), https://internetassociation.org/120215tcpa; *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits*, Inst. for Legal Reform (Aug. 2017), https://www.instituteforlegalreform.com/research/tcpa-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits.

29 *Melito v. Experian Mktg. Solutions, Inc.,* No. 17-3277-cv(L), 2019 WL 1906087, at *5 (2d Cir. Apr. 30, 2019).

30 *Second Circuit Holds Receipt of Unwanted Text Messages, Even Without Other Alleged Harm, Confers Standing for TCPA Claims*, Nat'l L. Rev. (May 17, 2019), https://www.natlawreview.com/article/second-circuit-holds-receipt-unwanted-text-messages-even-without-other-alleged-harm.

31 Fed. Comms. Comm'n, TCPA Omnibus Declaratory Ruling and Order, 30 F.C.C. Rcd. 7961 (10) (Oct. 9, 2015), available at https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order; TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits, *supra* n.28.

32 *Id.* (explaining that TCPA litigation increased by 46 percent following the FCC's 2015 Order).

33 Notably, questions regarding what qualifies as an automatic telephone dialing system (ATDS), or autodialer, multiplied following the FCC's 2015 Order. This remains a topic in great need of appropriate clarification from the FCC. In June 2019, a unanimous Ninth Circuit panel overturned dismissal of a TCPA class action, holding that security notification text messages were sent using an ATDS. *Duguid,* 2019 WL 2454853.

34 *Id.*

35 *WebRecon Stats for Mar. 2019: Upside Down & Inside Out,* Web Recon, https://webrecon.com/webrecon-stats-for-mar-2019-%E2%80%8Bupside-down-inside-out (last visited July 2, 2019).

36 *WebRecon Stats for April 2019: Lawsuits Up, YTD Trends Remain the Same*, Web Recon, https://webrecon.com/webrecon-stats-for-april-2019-lawsuits-up-ytd-trends-remain-the-same (last visited July 2, 2019).

37 *WebRecon Stats for May 2019: FCRA Down, Everything Else Up (And The Unexpected Resurgence of a Familiar Name)*, Web Recon, https://webrecon.com/webrecon-stats-for-may-2019-fcra-down-everything-else-up-and-the-unexpected-resurgence-of-a-familiar-name (last visited July 2, 2019).

38 *See, e.g., Williams v. Bluestem Brands, Inc.,* No. 8:17-cv-1971-T-27AAS, 2019 WL 1450090, at *2 n.2 (M.D. Fla. 2019); *see also Couser v. Comenity Bank,* 125 F. Supp. 3d. 1034, 1045 (S.D. Cal. 2015) (finding a 7.7 percent claim rate to be "higher than average"); *Hashw v. Dep't Stores Nat'l Bank,* 182 F. Supp. 3d 935, 945 (D. Minn. 2016) (noting that a 20% claim rate was "relatively high").

39 *Lee v. Global Tel*Link Corp.,* No. 2:15-cv-02495-ODW (PLA), 2018 WL 4625677, at *7 (C.D. Cal. 2018) (approving 1.8 percent claim rate settlement).

40 *See, e.g., Kolinek v. Walgreen Co.,* 311 F.R.D. 483, 493 (N.D. Ill. 2015) (approving an $11 million TCPA settlement, which when divided by the approximately 2.5 percent of claiming class members led to a pre-fee payment of $30 per claimant, and a post-fee payment of $21.83 per claimant).

41 *See, e.g., Mahoney v. TT of Pine Ridge, Inc.,* 2017 U.S. Dist. LEXIS 217470 (S.D. Fla. 2017) (granting TCPA settlement for $15 voucher or $4 cash); *Manouchehri v. Styles for Less, Inc.,* 2016 U.S. Dist. LEXIS 80038 (S.D. Cal. 2016) (granting TCPA settlement for $15 voucher or $10 cash award); *Anthony Oliver v. The Men's Wearhouse, Inc.,* Law360 (Aug. 22, 2018), https://www.law360.com/articles/1075649/men-s-wearhouse-agrees-to-settle-robotext-

suit-for-1-8m (awarding $20 voucher with $10 cash value); *Lennartson v. Papa Murphy's Int'l LLC,* Law360 (Apr. 24, 2018), https://www.law360.com/articles/1036548/pizza-chain-settles-consumers-tcpa-suit-for-22-6m (providing $10 voucher and $10 cash).

42 *See, e.g., Aranda v. Caribbean Cruise Line, Inc.,* No. 12-C4069, 2017 WL 818854 (N.D. Ill. Mar. 2, 2017) ("Plaintiffs' counsel have requested a fee award of 33% of the fund (minus notice expenses), up to a maximum of $24.5 million ... .").

43 *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits* at 29 n.13, *supra* n.28.

44 *See, e.g., Abante Rooter & Plumbing, Inc., et al. v. Alarm.com, Inc., et al.,* no. 4:15-cv-06314-YGR (ECF No. 295) (Mar. 18, 2019) (seeking $8.4 million in attorneys' fees, from a $28 million settlement fund).

45 *A Summary of Your Rights Under the Fair Credit Reporting Act,* https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf (last visited July 2, 2019).

46 *Fair Credit Reporting Act,* Fed. Trade Comm'n, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited July 2, 2019).

47 *Bulletin: FCRA Litigation on the Rise!,* Nat'l L. Rev. (Nov. 30, 2018), https://www.natlawreview.com/article/bulletin-fcra-litigation-rise.

48 *Id.*

49 136 S. Ct. 1540.

50 *Id.* at 1550.

51 *Id.*

52 *Robins v. Spokeo, Inc.,* 867 F.3d 1108, 1114 (9th Cir. 2017); *see also Stokes v. Realpage, Inc.,* Nos. 15-1520, 15-3894, 2015 WL 6095810, at *7 (E.D. Penn. Oct. 19, 2016).

53 15 U.S.C. § 1681 (providing for actual damages or statutory damages, punitive damages, the costs of the action, and attorney's fees).

54 *See, e.g., Esomonu v. Omnicare, Inc.,* No. 15-CV-02003-HSG, 2019 WL 499750, at *4 (N.D. Cal. Feb. 8, 2019) (approving FCRA settlement where claimants would receive approximately $17 per person, an amount "substantially below the range of potential statutory damages, but commensurate with recoveries approved by other California district courts" in the amount of $5 to $30 per person, $15 per person, and $41.39 per person).

55 *Eichenberger v. ESPN, Inc.,* 876 F.3d 979, 984 n.2 (9th Cir. 2017) ("Congress enacted the VPPA after a newspaper published Supreme Court nominee Robert Bork's video rental history. Notably, Judge Bork's rental history was decidedly commonplace, and the article did not hurt his nomination.")

56 *See, e.g., id.* at 983 (holding that "every disclosure of an individual's 'personally identifiable information' and video-viewing history offends the interests that the statute protects").

57 *Yershov v. Gannet Satellite Info. Network, Inc.,* 820 F.3d 482 (1st Cir. 2016).

58 *Id.*

59 *Eichenberger,* 876 F.3d 979, 986 (9th Cir. 2017).

60 *Id.*

61 *Id.* at 985 (citing *In re Nickelodeon Consumer Privacy Litig.,* 827 F.3d 266, 267 (3d Cir. 2016)).

62 *Id.*

63 740 Ill. Comp. Stat. 14/15.

64 740 Ill. Comp. Stat. 14/1 et seq.

65 740 Ill. Comp. Stat. 14/20(1) & (2).

66 *Rosenbach v. Six Flags Entm't Corp.,* 2019 IL 123186 (Ill. Jan. 25, 2019).

67 *See, e.g., Google Takes Aim at Controversial, Stringent Illinois Biometric Privacy Law,* One World Identity (Apr. 25, 2018), https://oneworldidentity.com/google-takes-aim-controversial-stringent-illinois-biometric-privacy-law (explaining that "the popular Google Arts & Culture app, which uses facial recognition algorithms ... was not released in Illinois because of the BIPA law" and "Nest—which is also owned by Alphabet—does not offer facial recognition capabilities in its doorbell camera in Illinois due to the local law, despite the fact that residents in other

states can access that capability"); *Want This Cute Robot Dog? Tough – Illinois Law Keeps Sony From Selling It Here,* Chicago Sun Times (Nov. 15, 2018), https://chicago.suntimes.com/2018/11/15/18315253/want-this-cute-robot-dog-tough-illinois-law-keeps-sony-from-selling-it-here (describing how Sony's robotic pup, Aibo, uses "his computer brain [to look] at people's faces, and can tell the difference between members of a household and play with them in different ways," which prompted Sony not to offer the robot in BIPA territory).

68 Gabe Friedman, *First Settlement Reached Under Illinois Biometric Law,* Bloomberg Law (Dec. 5, 2016), https://biglawbusiness.com/first-settlement-reached-under-illinois-biometric-law.

69 *Illinois Supreme Court Holds No Showing of Actual Harm Needed to State Claim Under Biometric Information Privacy Act,* Lexology (Jan. 28, 2019), https://oneworldidentity.com/google-takes-aim-controversial-stringent-illinois-biometric-privacy-law; BIPA Docket Alerts, Bloomberg Law (2019).

70 *Rosenbach,* 2019 IL 123186, at *10-11.

71 740 Ill. Comp. Stat. 14/20 (providing for per violation liquidated damages or actual damages, attorneys' fees and costs, and other relief as the court deems appropriate).

72 *In re Facebook Biometric Info. Priv. Litig.,* 326 F.R.D. 535 (N.D. Cal. 2018), *appeal docketed,* No. 18-15982 (9th Cir. May 30, 2018).

73 Dorothy Atkins, *Facebook Asks 9th Circ. To Decertify Class In Face Scan Suit,* Law360 (June 12, 2019), https://www.law360.com/technology/articles/1168482/facebook-asks-9th-circ-to-decertify-class-in-face-scan-suit.

74 Cal. Civ. Code § 1798.140(o)(1)(E) (West 2019); Conn. Gen. Stat. § 38a-999b(a)(4) (West 2019); Conn. Gen. Stat. § 53a-129a (West 2019); Mass. Gen. Laws ch. 93I, § 1 (West 2019); 6 R.I. Gen. Laws § 6-52-1(3) (West 2019).

75 *See, e.g., Id.*

76 Cal. Civ. Code § 1798.140(o)(1)(E) (West 2019) ("Personal information includes ... biometric information."); *Id.* at § 1798.150(a)(1).

77 Tex. Bus. & Com. Code Ann. § 503.001; 19 Wash. Rev. Code 375.

78 Tex. Bus. & Com. Code Ann. § 503.001(d); 19 Wash. Rev. Code 375.030(2).

79 Torsten Kracht et al., *Biometric Information Protection: The Stage Is Set for Expansion of Claims*, LexisNexis (Feb. 28, 2018), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/posts/biometric-information-protection-the-stage-is-set-for-expansion-of-claims; Chris Burt, *Florida Considers Biometric Data Privacy Law with Private Action Rights Like BIPA,* Biometric Update.com (Mar. 4, 2019), https://www.biometricupdate.com/201903/florida-considers-biometric-data-privacy-law-with-private-action-rights-like-bipa; Issie Lapowsky, *New York's Privacy Bill is Even Bolder Than California's,* Wired (June 4, 2019, 7:00 AM), https://www.wired.com/story/new-york-privacy-act-bolder.

80 H.R. 2478, 54th Leg., 1st Reg. Sess. (Ariz. 2019); H.R. 645, 66th Leg., Reg. Sess. (Mont. 2019); *Several States Considering Laws Regulating the Collection of Biometric Data,* Lexology (Feb. 6, 2019), https://www.lexology.com/library/detail.aspx?g=a545aec6-37b8-49a8-8487-74b61883a0e1.

81 *See, e.g., Gardner v. Health Net, Inc.,* No. CV 10-2140PA(CWx), 2010 WL 11597979 (C.D. Cal. Aug. 12, 2010).

82 *Id.*

83 *Id.*

84 *Id.* at *10 (internal citation omitted).

85 30 days prior to filing suit, consumers must provide written notice to would-be defendants, and an opportunity to cure. Cal. Civ. Code § 1798.150(b)(1) (West 2019).

86 *Id.* at § 1798.150.

87 *Id.* at § 1798.150(a)(1)(A).

88 *Id.* at 1798.150(a)(B) & (C).

89 David Strauss, *CCPA: Bill to Expand Private Right of Action Fails,* JDSupra (May 17, 2019), https://www.jdsupra.com/legalnews/ccpa-bill-to-expand-private-right-of-65974.

90 *Id.*

91 *See, e.g., International Collaboration To Protect Children's Privacy,* Fed. Trade Comm'n (May 11, 2015) ("The Federal Trade Commission [which enforces COPPA] and 27 members of the

Global Privacy Enforcement Network (GPEN), a group of privacy enforcement agencies around the world, are marshaling resources to protect the privacy of children online ... In this latest initiative, privacy experts from the FTC's Office of Technology Research and Investigation will conduct an analysis of the privacy disclosures, interactive features, and information collection practices of children's mobile apps.").

92 *Compare Meyers v. Nicolet Rest. of De Pere, LLC,* 843 F.3d 724 (7th Cir. 2016), *cert. denied,* 137 S. Ct. 2267 (2017) (holding that a restaurant's violation of the Fair and Accurate Credit Transactions Act (FACTA) by failing to truncate the expiration date of a customer's credit card on a receipt did not create an injury in fact), *with Jeffries v. Volume Servs. Amer. Inc., et al.,* No. 1:17-cv-01788 (D.C. Cir. July 2, 2019) (holding that a receipt printed by a concessionaire containing all 16 digits of a customer's credit card number was an "egregious" violation of FACTA sufficient to confer standing), *and Wood v. J Choo U.S.A., Inc.,* 201 F. Supp. 3d 1332, 2340 (S.D. Fla. 2016) (holding that Congress created a substantive legal right for cardholders under FACTA, and that consumers suffer a concrete and particularized harm "as soon as" an offending credit card receipt is printed).

93 *The Future of Cybersecurity Insurance and Litigation: An Interview with Kimberly Horn,* Teach Privacy (Oct. 9, 2018), https://teachprivacy.com/future-of-cybersecurity-insurance-litigation-kimberly-horn (interviewing the Global Focus Group Leader for Cyber Claims at Beazley (insurance), who explained, "Not all data breaches are created equal, and the facts that form the foundation of some of the most widely publicized breaches do not easily lend themselves to cognizable damages, yet there is a great deal of variation in how the federal judiciary applies the litmus test for Article III standing in data breach class action litigation").

94 *See supra* at p. 8 (describing the minimal payments received by class members, if any, resulting from class action settlements).

95 *Nest's Newest Home-Security Camera Will Use Facial Recognition To Identify Those It Records,* L.A. Times (May 31, 2017), https://www.latimes.com/business/la-fi-tn-nest-facial-recognition-20170531-story.html (explaining that Illinois residents will not have the option to use Nest Lab's facial recognition technology in the home security camera, which in other states helps monitor children arriving home from school, or the presence of other individuals at the home).

96 *WebRecon Stats for April 2019: Lawsuits Up, YTD Trends Remain the Same,* Web Recon (May 8, 2019), https://webrecon.com/webrecon-stats-for-april-2019-lawsuits-up-ytd-trends-remain-the-same (noting that approximately 32 percent of plaintiffs who filed suit in April 2019 under various federal statutes had previously served as plaintiffs, and a "FCRA attorney ... retains the crown for most lawsuits of the year, with 154 consumers represented").

97 Amy Korte, *While Illinois Courts Amazon, Privacy Litigation Threatens Tech Firms, Illinois Employers,* Illinois Policy (Oct. 27, 2017), https://www.illinoispolicy.org/while-illinois-courts-amazon-privacy-litigation-threatens-tech-firms-illinois-employers.

98 42 U.S.C.A. § 1302 *et seq.* (West 2019).

99 15 U.S.C.A. §§ 6501-6506 (West 2019).

100 20 U.S.C.A. § 1232g *et seq.* (West 2019).

101 40 U.S.C.A. § 2000ff *et seq.* (West 2019).

102 *About Us (OCR),* Office for Civil Rights, https://www.hhs.gov/ocr/about-us/index.html (last visited July 2, 2019).

103 *Enforcement Highlights,* HHS.gov, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (last visited July 2, 2019).

104 *Id.; see also HIPAA Violations & Enforcement,* Am. Med. Ass'n, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement (last visited July 2, 2019) (noting that HIPAA violations can result in civil or criminal penalties).

105 *Id.*

106 *Id.*

107 *Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties*, Fed. Register (Apr. 30, 2019), https://www.federalregister.gov/documents/2019/04/30/2019-08530/

notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties (describing that these penalties are adjusted for inflation).

108 *See, e.g., HIPAA Fines Listed by Year,* Compliancy Grp., https://compliancy-group.com/hipaa-fines-directory-year (last visited July 2, 2019) (listing fines imposed by OCR under HIPAA from 2015 through 2018, ranging from $31,000 to $16,000,000).

109 *Cases Currently Under Investigation,* U.S. Dep't for Health and Human Servs. Office for Civ. Rights (last visited July 2, 2019), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

110 *App Stores Remove Three Dating Apps After FTC Warns Operator About Potential COPPA, FTC Act Violations,* Fed. Trade Comm'n (May 6, 2019), https://www.ftc.gov/news-events/press-releases/2019/05/app-stores-remove-three-dating-apps-after-ftc-warns-operator.

111 Sheila Millar & Tracy Marshall, *New Enforcement Actions for COPPA's 20th Anniversary,* Law360 (Jan. 3, 2019), https://www.law360.com/articles/1114765/new-enforcement-actions-for-coppa-s-20th-anniversary.

112 *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That It Violated Children's Privacy Law,* Fed. Trade Comm'n (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

113 *Id.*

114 *App Stores Remove Three Dating Apps After FTC Warns Operator About Potential COPPA, FTC Act Violations, supra* n.110.

115 *Id.*

116 *Id.*

Notes

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com