2021

Privacy Harms

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Danielle Keats Citron
University of Virginia School of Law, keatsmorris@gmail.com

PRIVACY HARMS

by

Danielle Keats Citron
& Daniel J. Solove

PRIVACY HARMS

by Danielle Keats Citron[*]
& Daniel J. Solove[**]

[*] Jefferson Scholars Foundation Schenck Distinguished Professor of Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow.
[**] John Marshall Harlan Research Professor of Law, George Washington University Law School. We would like to thank research assistants Kimia Favagehi, Katherine Grabar, Jean Hyun, Austin Mooney, and Julia Schur.

ABSTRACT

Privacy harms have become one of the largest impediments in privacy law enforcement. In most tort and contract cases, plaintiffs must establish that they have been harmed. Even when legislation does not require it, courts have taken it upon themselves to add a harm element. Harm is also a requirement to establish standing in federal court. In Spokeo v. Robins, *the U.S. Supreme Court has held that courts can override Congress's judgments about what harm should be cognizable and dismiss cases brought for privacy statute violations.*

The caselaw is an inconsistent, incoherent jumble, with no guiding principles. Countless privacy violations are not remedied or addressed on the grounds that there has been no cognizable harm. Courts conclude that many privacy violations, such as thwarted expectations, improper uses of data, and the wrongful transfer of data to other organizations, lack cognizable harm.

Courts struggle with privacy harms because they often involve future uses of personal data that vary widely. When privacy violations do result in negative consequences, the effects are often small – frustration, aggravation, and inconvenience – and dispersed among a large number of people. When these minor harms are done at a vast scale by a large number of actors, they aggregate into more significant harms to people and society. But these harms do not fit well with existing judicial understandings of harm.

This article makes two central contributions. The first is the construction of a road map for courts to understand harm so that privacy violations can be tackled and remedied in a meaningful way. Privacy harms consist of various different types, which to date have been recognized by courts in inconsistent ways. We set forth a typology of privacy harms that elucidates why certain types of privacy harms should be recognized as cognizable. The second contribution is providing an approach to when privacy harm should be required. In many cases, harm should not be required because it is irrelevant to the purpose of the lawsuit. Currently, much privacy litigations suffers from a misalignment of law enforcement goals and remedies. For example, existing methods of litigating privacy cases, such as class actions, often enrich lawyers but fail to achieve meaningful deterrence. Because the personal data of tens of millions of people could be involved, even small actual damages could put companies out of business without providing much of value to each individual. We contend that the law should be guided by the essential question: When and how should privacy regulation be enforced? We offer an approach that aligns enforcement goals with appropriate remedies.

I. INTRODUCTION

Harm has become one of the biggest challenges in privacy law.[1] Law's treatment of privacy harms is a jumbled, incoherent mess. Countless privacy violations are left unaddressed because courts refuse to recognize harm that has been suffered. As Ryan Calo has observed, "courts and some scholars require a showing of harm in privacy out of proportion with other areas of law."[2]

Privacy law in the United States is a sprawling patchwork of various types of law, from contract and tort to statutes and other bodies of law.[3] As these laws are enforced, especially in the courts, harm requirements stand as a major impediment. When cases are dismissed due to the lack of harm, organizations engaging in wrongdoing escape without accountability. The message to other organizations is both clear and troubling—they can ignore privacy commitments enshrined in legislation and common law without concern.

In several ways, harm emerges as a key gatekeeper in privacy cases. Harm is an element of many causes of action. Courts struggle to recognize privacy harms because they often do not produce tangible financial or physical harm.[4] Instead, privacy harms often involve intangible injuries, which courts address inconsistently and with considerable disarray. Many privacy violations involve broken promises or thwarted expectations about how people's data will be collected, used, and disclosed. The downstream consequences of these practices are often hard to determine in the here and now. People might be flooded with unwanted advertising or email spam. Their expectations may be betrayed, resulting in their data being shared with third parties that may use it in detrimental ways –but precisely when and how is unknown.

For many privacy harms, the injury may appear small when viewed in isolation, such as the inconvenience of receiving an unwanted email or advertisement or the failure to honor your expectation that your data would not be shared with third parties. But when done by hundreds or thousands of companies, the harm adds up. Moreover, these small harms are dispersed among millions (and sometimes billions) of people. Over time, as numerous people are each

---

[1] Jacqueline D. Lipton, *Mapping Online Privacy*, 104 Nw. U. L. Rev. 477, 508 (2010) ("Delineating remediable harms has been a challenge for law and policy makers since the early days of the Internet.").

[2] Ryan Calo, *Privacy Harm Exceptionalism*, 12 Colo. Tech. L.J. 361, 361 (2014); *see also* Ryan Calo, *Privacy Law's Indeterminacy*, 20 Theoretical Inquiries L. 33, 48 (2019) (Courts "do not understand privacy loss as a cognizable injury, even as they recognize ephemeral harms in other contexts").

[3] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (7th ed. 2021).

[4] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 798-99 (2016) ("For most courts, privacy and data security harms are too speculative and hypothetical, too based on subjective fears and anxieties, and not concrete and significant enough to warrant recognition.").

inundated by a swarm of small harms, the overall societal impact can be significant. Yet, these types of injuries do not fit well into judicial conceptions of harm, which have an individualistic focus and heavily favor tangible physical and financial injuries that occur immediately.

Some statutory laws recognize government agency or state attorney general enforcement that are less constrained by judicial conceptions of harm, but these enforcers have limited resources so can only bring a handful of actions each year.[5] To fill the anticipated enforcement gap, legislators have often included statutory private rights of action. The financial rewards of litigating and winning cases work like a bounty system, encouraging private parties to enforce the law.[6] To address the difficulties in establishing privacy harms, several privacy statutes contain statutory damages provisions, which allow people to recover a minimum amount of money without having to prove harm.

Courts, however, have wrought havoc on legislative plans for statutory damages in privacy cases by adding onerous harm requirements. In *Doe v. Chao*, for example, the Supreme Court held that a statutory damages provision under the federal Privacy Act of 1974 would only impose such damages if plaintiffs established "actual" damages.[7] As a second punch, the Supreme Court held in *Federal Aviation Administration v. Cooper* that emotional distress alone was insufficient to establish actual damages under the Privacy Act.[8] In a variation of this theme, in *Senne v. Village of Palatine*,[9] the U.S. Court of Appeals for the Seventh Circuit held that a plaintiff had to prove harm to recover under a private right of action for a violation of the federal Driver's Privacy Protection Act even though the provision lacked any harm requirement.

Courts have also injected harm as a gatekeeper to the enforcement of the law through modern standing doctrine. The U.S. Supreme Court has held that plaintiffs cannot pursue cases in federal court unless they have suffered an "injury in fact."[10] Specifically, in the privacy law context, in 2016, the Supreme Court in *Spokeo v. Robins*, concluded in a case involving the Fair Credit Reporting Act that courts could deny standing to plaintiffs seeking to recover under private rights of action in statutes. The court stated that even if a legislature granted plaintiffs a right to recover without proving harm, courts

[5] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 799 (2016) ("Federal authorities cannot attend to most privacy and security problems because their resources are limited and their duties ever expanding. Simply put, federal agencies have too few resources and too many responsibilities.")

[6] *See* Crabill v. Trans Union, LLC, 259 F.3d 662, 665 (7th Cir. 2001) (noting that "[t]he award of statutory damages could also be thought a form of bounty system, and Congress is permitted to create legally enforceable bounty systems for assistance in enforcing federal laws.").

[7] 540 U.S. 614, 614 (2004). Id. at 614.

[8] 132 S. Ct. 1441 (2012).

[9] 695 F.3d.597 (7th Cir. 2015).

[10] Friends of the Earth Inc. v. Laidlaw Envt'l Sys. (TOC), Inc., 528 U.S. 167 (2000).

could require a plaintiff to prove harm to establish standing.[11]

Due to judicial intervention, the requirement of privacy harm is inescapable. Even when law does not require proof of harm, courts exert their will to add it in, turning the enforcement of privacy law into a far more complicated task than it should be. Privacy harm is a conceptual mess, obscured in a fog that significantly impedes U.S. privacy law from being effectively enforced. Even when organizations have engaged in clear wrongdoing, privacy harm requirements often result in cases being dismissed.

In this Article, we clear away the fog so that privacy harms can be better understood and appropriately addressed.[12] We set forth a typology that explains why particular harms should be legally cognizable. We show how concepts and doctrines in other areas of law can be applied in the context of privacy harms.

A better understanding and recognition of privacy harms is only the first part of the equation. In addition to the issue of *what should constitute cognizable privacy harm*, we also examine the issue of *when privacy harm should be required*. In many cases, harm should not be required because it is irrelevant to the purpose of the lawsuit. The overarching question that the law should ask is: *When and how should various privacy laws be enforced?* This question brings into focus the underlying source of the law's current malaise—the misalignment of enforcement goals and remedies. We propose an approach that aligns enforcement goals with appropriate remedies.

This Article has four parts. Part I discusses when the law requires cognizable harm in order to enforce privacy regulation. Part II sets forth a typology of privacy harms, explaining why each involves an impairment of important interests, how law tackles them, and why the law should do so. Part III examines several challenges that make it difficult to recognize certain types of privacy harms. Part IV examines when privacy harm should be required in privacy litigation and how the law should better align enforcement goals and remedies.

[11] 136 S. Ct. 1540 (2016).

[12] Previously, we wrote an article about data breach harms. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Tex. L. Rev. 737 (2018). We write separately on privacy harms because they are quite different. Data breach harms often involve either anxiety or a risk of future identity theft or fraud. Privacy harms are more varied than data breach harms and involve many other dimensions that pose challenges for the law.

I. COGNIZABLE HARMS: THE LEGAL RECOGNITION OF PRIVACY HARMS

Requirements to establish harm serve as a major hurdle in privacy cases. Harms involve an injury, setback, loss, or impairment to well-being.[13] They leave people or society worse off than before their occurrence. Frequently, establishing harm is a prerequisite to the enforcement for privacy violations in the judicial system. A *cognizable harm* is a harm that the law recognizes based on the law's conception of harm.[14]

Through harm requirements, courts have made the enforcement of privacy laws difficult, and, at times, impossible. They have added requirements for harm via standing. They have required harm for statutes that do not require such a showing. They have mandated proof of harm even for statutes that include statutory damages, undercutting the purpose of these provisions. They have adopted narrow conceptions of cognizable harm to exclude many types of harm, including emotional injury and dashed expectations. Because courts lack a theory of privacy harms or any guiding principles, they have made a mess of things. This Part discusses the varied ways that harm is involved in privacy cases.

A. STANDING

To pursue a lawsuit in federal court, a plaintiff must have standing. Standing is based on Article III of the U.S. Constitution, which states that courts are limited to hearing "cases" or "controversies."[15] In a series of cases starting in the second half of the Twentieth Century, the U.S. Supreme Court has placed harm at the center of standing.[16] State courts generally do not require proof of standing.

The U.S. Supreme Court has developed a rather tortured body of standing doctrine, which is restrictive in its view of harm as well muddled and contradictory. Under contemporary standing doctrine, plaintiffs must allege an "injury in fact."[17] The injury must be "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[18] If a plaintiff lacks standing to bring a claim, a federal court cannot hear it. Two cases decided during the past

---

[13] A taxonomy of privacy developed by one of us focused on privacy *problems*. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008). Problems are broader than harms. Problems are undesirable states of affairs. Harms are a subset of problems.

[14] JOEL FEINBERG, HARM TO OTHERS: THE MORAL LIMITS OF CRIMINAL LAW 34 (1984); see also OLIVER WENDELL HOLMES, THE COMMON LAW 64 (1881, reissued 1963); Thomas C. Grey, *Accidental Torts*, 54 Vand. L. Rev. 1225, 1272 (2001) (discussing Holmes's harm-based approach).

[15] U.S. Const. Art. I.

[16] Friends of the Earth Inc. v. Laidlaw Envt'l Sys. (TOC), Inc., 528 U.S. 167 (2000).

[17] Friends of the Earth Inc. v. Laidlaw Envt'l Sys. (TOC), Inc., 528 U.S. 167 (2000); *Lujan v. Defenders of Wildlife,* 504 U.S. 555 (1992).

[18] Id.

decade focused on privacy issues.

In 2013, in *Clapper v. Amnesty International*,[19] a group of lawyers, journalists, and activists challenged the constitutionality of surveillance by the National Security Agency (NSA). The plaintiffs contended that because they were communicating with foreign people who were likely to be considered suspicious by the NSA, they feared their communications would be wiretapped. The plaintiffs thus took measures to avoid the surveillance and maintain attorney-client confidentiality, such as traveling in person to have client discussions.[20] The Court held that the plaintiffs lacked standing because they failed to prove that they were actually under surveillance or that surveillance was "certainly impending." The plaintiffs' "speculation" about being under surveillance was insufficient.[21] In a footnote, the Court noted that, "in some instances," a "substantial risk that the harm will occur would be sufficient to confer standing to plaintiff."[22] The Court never explained what would constitute a "substantial risk."

Although *Clapper* has had a significant impact on data breach cases, a subsequent case has taken center stage for standing in privacy cases. In 2016, in *Spokeo, Inc. v. Robins*, the Supreme Court attempted to elaborate on the types of harm that could be sufficient to establish standing.[23] The Court focused on whether statutory violations involving personal data constituted harm sufficient to establish standing. The plaintiff alleged that Spokeo, a site supplying information about people's backgrounds, violated the federal Fair Credit Reporting Act (FCRA) when it published incorrect data about him.[24] Spokeo's profiles were used by employers to investigate prospective hires, an activity regulated by the FCRA. The FCRA mandates that firms take reasonable steps to ensure the accuracy of data in people's profiles.[25] The plaintiff's dossier was riddled with falsehoods, including that he was wealthy, married, had children, and worked in a professional field.[26] According to the plaintiff, these errors hurt his employment chances by indicating that he was overqualified for positions he

[19] 133 S. Ct. 1138 (2013).
[20] For a thoughtful analysis of *Clapper*, *see* Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013).
[21] The *Clapper* case comes with a dose of cruel irony. Although the government diminished the plaintiffs' concerns about surveillance by arguing that the plaintiffs could not prove that they were subject to it, the government knew the answer all along, but because the program was classified as a state secret, the plaintiffs did not and could not know for sure that they were being subject to surveillance. *See* Seth F. Kreimer, *"Spooky Action at a Distance:" Intangible Injury in Fact in the Information Age*, 18 U Pa. J. Con. L. 745, 757 (2016).
[22] *Id.* at 1150 n.5. In *Susan B. Anthony List v. Driehaus*, the Court, quoting *Clapper*, held that "an allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." 134 S. Ct. 2334, 2341 (2014).
[23] 136 S. Ct. 1540 (2016).
[24] *Id.* at 1544.
[25] 15 U.S.C. § 1681.
[26] *Id.* at 1546.

sought or that he might have difficulty relocating because he had a family.[27]

Although the plaintiff properly sued under FCRA's private right of action, according to the district court, the plaintiff lacked standing because he had not suffered an injury based on the erroneous information.[28] The U.S. Court of Appeals for the Ninth Circuit reversed on the grounds that the statute resolved the question of whether a cognizable injury existed: FCRA explicitly allowed plaintiffs to sue for any violation of FCRA.[29]

The U.S. Supreme Court took up the case, issuing an opinion purporting to clarify standing doctrine but instead creating significant confusion. Instead of deferring to Congress's judgment for when plaintiffs could sue for violations of the FCRA, the Court added harm into the equation through standing. Reversing and remanding the case back to the Ninth Circuit, the Court explained that harm must be "concrete" and that "intangible harm" could be sufficient in some cases to establish injury.[30] According to the Court, a "real risk of harm" could satisfy the concreteness because long-standing common law has "permitted recovery by certain tort victims even if their harms may be difficult to prove or measure."[31] The question would turn on "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[32] Unfortunately, the common law invoked by the Court points in different directions. The Court's discussion of "intangible harm" ended up creating confusion rather than clarity.

The Court confounded matters in yet another way—it instructed courts to assess the judgment of Congress" to figure out "intangible harm constitutes injury in fact."[33] The Court began by noting:

> [W]e said in *Lujan* that Congress may 'elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.' Similarly, Justice Kennedy's concurrence in that case explained that 'Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.'[34]

Although Congress could independently define "concrete injury" in a way that enlarged the concept, the Court also said that Congress could deviate only so

---

[27] *Id*. at 1556 (Ginsburg, J., dissenting).
[28] *Id*.at 1546.
[29] Robins v. Spokeo, Inc., 742 F.3d 409, 411–14 (9th Cir. 2014), *vacated* 136 S. Ct. 1540 (2016). See FCRA, 15 U.S.C. § 1681n (willful violations), and 15 U.S.C. § 1681o (negligent violations).
[30] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).
[31] *Id*. at 1549.
[32] *Id*. at 1549.
[33] *Id*. at 1549.
[34] *Id*. at 1549 (citations omitted).

much:

> Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.[35]

As to how far Congress could deviate from courts in defining injuries, the Court failed to provide a clear answer. As an example, the Court noted that courts could reject a "bare procedural violation" of a statute as an injury, but this example was muddled with further explanation:

> [T]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified.[36]

The Court thus said on one hand that a mere violation of a procedural right *can* be sufficient for concrete injury "without any *additional* harm." But, on the other hand, a "bare procedural violation, divorced from any concrete harm" cannot constitute concrete harm. So, how are courts to distinguish between when a violation of a procedural right is a concrete injury and when it is not?

The Court tried to explain its reasoning by noting that Congress passed the FCRA "to curb the dissemination of false information," so bare procedural violations would not support standing if they did not operate to prevent such inaccuracies.[37] The Court explained that consumers may not be able to sue a consumer reporting agency for failing to provide notice required by the statute if the information in their dossiers was accurate.[38] The Court further complicated matters by stating that "not all inaccuracies cause harm or present any material risk of harm." The example provided by the Court was an incorrect zip code. The Court explained, "It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[39]

The Court remanded the case to the Ninth Circuit to "examine whether the particular procedural violations alleged in this case entail a degree of risk

---

[35] *Id.* at 1549
[36] *Id.* at 1549
[37] *Id.* at 1550.
[38] *Id.* at 1550.
[39] *Id.* at 1550.

sufficient to meet the concreteness requirement."[40] The Court noted that it was not taking a particular position about whether Robins properly alleged an injury.

In the wake of *Spokeo,* courts have issued a contradictory mess of decisions regarding privacy harm and standing. The Ninth Circuit concluded that Robins had suffered harm, justifying standing.[41] The court applied a test from the Second Circuit that assessed whether a statutory provision was designed to protect people's concrete interests and whether those interests were at risk of harm in a particular case.[42] Other courts have extracted a two-prong test from the wreckage of *Spokeo,* first looking to "historical inquiry" that "asks whether an intangible harm 'has a close relationship' to one that historically has provided a basis for a lawsuit," and second, looking to a "congressional inquiry" that "acknowledges that Congress's judgment is 'instructive and important' because that body 'is well positioned to identify intangible harms that meet minimum Article III requirements.'"[43]

Ultimately, no clear principles have emerged to guide the harm inquiry for standing in privacy cases. Rather than a circuit split or other clear disagreement in approach, what we have is a mess. Under the post-*Spokeo* jurisprudence, it is unclear how courts are assessing intangible injuries in privacy cases. On the whole, decisions take a stab by grasping at inconsistent parts of *Spokeo.*[44]

Predictably, courts are reaching opposing conclusions as to the very same or similar FCRA violations. In *Dutta v. State Farm Mutual Auto Insurance Co.*, the Ninth Circuit concluded that violating FCRA by failing to provide the plaintiff with a copy of his credit report before disqualifying him from the hiring process was not a harm. The court concluded that the plaintiff was not harmed because he was disqualified by the correct information in the credit report.[45] By contrast, in *Long v. Southeastern Pennsylvania Transportation Authority,* the Third Circuit denied standing to a plaintiff suing under FCRA for not being provided with his background check before being rejected for a job.[46]

As the Third Circuit stated in another case involving a FCRA violation: "In some cases, we have appeared to reject the idea that the violation of a statute can, by itself, cause an injury sufficient for purposes of Article III standing. But we have also accepted the argument, in some circumstances, that the breach of a statute is enough to cause a cognizable injury — even without economic or other

[40] *Id.* at 1550.
[41] Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017), cert. denied, 138 S. Ct. 931 (2018).
[42] *Id.* at 1113 (citing Strubel v. Comenity Bank, 842 F.3d 181, 190 (2d Cir. 2016).
[43] Long v. Southeastern Pa. Transp. Auth., 903 F.3d 312, 321 (3d Cir. 2018) (quoting *Spokeo*).
[44] Jackson Erpenbach, Note, *A Post*-Spokeo *Taxonomy of Intangible Harms*, 118 Mich. L. Rev. 471, 483 (2019) (*Spokeo* has affected consumer protection laws unevenly. For example, while it risks extinguishing claims arising under FACTA, claims under TCPA are virtually unimpeded.").
[45] Dutta v. State Farm Mut. Auto. Ins. Co., 895 F.3d 1166 (9th Cir. 2018).
[46] Long v. Se. Pa. Transp. Auth., 903 F.3d 312, 316-17 (3d Cir. 2018).

tangible harm."[47] As the Sixth Circuit declared when it dismissed a case for lack of standing: "It's difficult, we recognize, to identify the line between what Congress may, and may not, do in creating an 'injury in fact.' Put five smart lawyers in a room, and it won't take long to appreciate the difficulty of the task at hand."[48]

B. HARM IN CAUSES OF ACTION

For plaintiffs in federal court, standing is just the first harm hurdle. The second is showing harm as an element of claims alleged in the lawsuit. In state courts, where there is no standing requirement, most causes of action have harm as one of the elements. Different types of causes of action recognize cognizable harm differently.

1. Contract Law

Contract law might seem to be a relevant body of law to regulate many privacy issues, as many privacy violations involve organizations breaking promises made in privacy policies. These policies could be deemed to be contracts or at the least subject to the doctrine of promissory estoppel. But, on the main, courts have been reluctant to recognize privacy policies as contracts.[49]

Even if privacy policies were contracts, the plaintiffs would still lose due to the absence of cognizable harm.[50] Under contract law, courts typically will not recognize harm without proof of economic loss. Failing to fulfill promises made in privacy policies and thus betraying people's expectations has been insufficient to constitute a cognizable harm.[51] For example, in *Smith v. Trusted Universal Standards In Elec. Transactions, Inc.*, the court stated that plaintiff must "plead loss flowing from the breach [of contract] to sustain a claim."[52] In

[47] In re Horizon Healthcare Data Breach, 846 F.3d 625, 635 (3d Cir. 2017).
[48] Hagy v. Demers & Adams, 882 F.3d 616, 623 (6th Cir. 2018).
[49] Courts have decided surprisingly few cases involving contract law theories for privacy notices. Of those cases, few have held that privacy policies amount to enforceable contracts. A group of academics published an empirical analysis of cases and concluded that many courts were holding that privacy notices were contracts. *See* Oren Bar-Gill et al., *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. Chi. L. Rev. 7 (2017). These academics used their study as part of their project with the American Law Institute, the Restatement of Consumer Contract Law. However, Gregory Klass critiqued the study, finding that the case holdings were incorrectly evaluated, treating issues in dicta or not addressed as definitive holdings. Klass found "little support" for any "trend towards contractual enforcement of privacy notices.'" Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 Yale J. on Reg. 45-115 (2019). A subsequent analysis of the Bar-Gill study sided with Klass. Adam J. Levitin et. al., *The Faulty Foundation of the Draft Restatement of Consumer Contracts*, 36 Yale J. on Reg. 447 (2019).
[50] *See infra* text accompanying notes.
[51] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877, 881-84, 892-3 (2003).
[52] Smith v. Trusted Universal Standards In Elec. Transactions, Inc., 2010 WL 1799456 (D.N.J. May 4, 2010).

Rudgayzer v. Yahoo! Inc., the court held that "[m]ere disclosure" of personal information "without a showing of actual harm" is "insufficient to support a claim of breach of contract."[53] In *In re Facebook Privacy Litig*ation, the court rejected plaintiffs' theory they suffered "appreciable and actual damage" in a suit for breach of contract."[54]

2. Tort Law

Most tort claims require that plaintiffs establish harm. As tort law developed in the nineteenth century, a lively debate centered on whether tort law concerned the recognition of wrongs or, alternatively, the redress of harms. In *The Common Law*, Oliver Wendell Holmes argued that tort law provided remedies for activities "not because they are wrong, but because they are harms.'[55] Modern tort law has embraced the Holmesian approach.[56]

The privacy torts grew out of Samuel Warren and Louis Brandeis's influential article in 1890, *The Right to Privacy*.[57] For students of their famous article, that result is odd given its rights-based focus on interferences with "individuals' ability to develop their 'inviolate' personalities without unwanted interference."[58] The judicial development of the privacy torts can be attributed to William Prosser, the leading torts scholar of the 20th century, who played an enormous role in mainstreaming and legitimizing the privacy torts.[59]

Prosser made the turn to harm explicitly and clearly, and courts followed suit. In 1960, in an article entitled *Privacy*, Prosser summed up a scattered body of caselaw to identify four torts: (1) intrusion upon the plaintiff's seclusion; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[60] As reporter on the influential American Law Institute's (ALI) Restatement (Second) of Torts, Prosser added the four categories of privacy torts to the Restatement.[61] Prosser followed the Holmesian harms-based approach in constructing the privacy

---

[53] Rudgayzer v. Yahoo! Inc., 5:12-CV-01399 EJD, 2012 WL 5471149 (N.D. Cal. Nov. 9, 2012), appeal dismissed (Dec. 13, 2012) (internal quotations omitted).
[54] *In re Facebook Privacy Litig*ation, C 10-02389 JW, 2011 WL 6176208 (N.D. Cal. Nov. 22, 2011).
[55] OLIVER WENDELL HOLMES, THE COMMON LAW 144 (1881).
[56] There is a robust and important literature on tort law as the recognition of wrongs. See JOHN C.P GOLDBERG & BENJAMIN ZIPURSKY, RECOGNIZING WRONGS (2020).
[57] Samuel L. Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[58] Danielle Keats Citron, *Mainstreaming Privacy Torts,* 98 Calif. L. Rev. 1805, 1820 (2010) (quoting Warren and Brandeis, *The Right to Privacy*).
[59] Danielle Keats Citron, *Mainstreaming Privacy Torts,* 98 Calif. L. Rev. 1805 (2010); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy,* 98 Cal. L. Rev. 1887 (2010).
[60] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[61] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy,* 98 Cal. L. Rev. 1887 (2010).

torts.[62] After Prosser's article and the Restatement, courts readily embraced the privacy torts.[63] Although Prosser strengthened the privacy torts, his work ossified them.[64] No new privacy torts were created in the years following Prosser's shining the spotlight on them.

Today, nearly all states recognize most of the privacy torts.[65] Courts rarely question the existence of harm or the fact that the basis of harm for many privacy torts is pure emotional distress. They tend to presume the existence of harm.[66] And yet while the privacy torts handily address the privacy problems of Warren and Brandeis's time, such as invasions of privacy by the media, this is not the case for modern privacy problems involving the collection, use, and disclosure of personal data. Because courts cling rigidly to the elements of the privacy torts as set forth in the Restatement, the privacy torts have little application to contemporary privacy issues.[67]

Other mainstream torts have been invoked to address privacy issues, such as intentional infliction of emotional distress, breach of confidentiality, and negligence. These torts are often limited by harm requirements, making it difficult for plaintiffs to obtain redress. For example, the intentional infliction of emotional distress tort requires proof of "severe emotional distress," which can be difficult to establish.[68]

3. Statutory Causes of Action

Many state and federal privacy statutes provide for private rights of action. Typically, the assumption is that a private right of action is a legislative recognition of harm, though there is no rule or doctrine that commands that all private rights of action in statutes are adopted to redress harm. Some might be there to facilitate private enforcement of a law or to deter violations.

---

[62] Citron, *Mainstreaming Privacy Torts, supra*, at 1821-24.
[63] Richards & Solove, *Prosser's Privacy Law, supre* note X, at 1903.
[64] *Id.* at 1904-07; G. EDWARD WHITE, TORT LAW IN AMERICAN HISTORY: AN INTELLECTUAL HISTORY (1980).
[65] Richards & Solove, *Prosser's Privacy Law, supre* note X, at 1904
[66] Solove & Citron, *Risk and Anxiety, supra* note X, at 768-70.
[67] Citron, *State Attorneys General, supra* note X, at 798 ("Overly narrow interpretations of the privacy torts--intrusion on seclusion, public disclosure of private fact, false light, and misappropriation of image--have prevented their ability to redress data harms.").
[68] RESTATEMENT (SECOND) OF TORTS § 46 (liability for "[o]ne who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another"). This tort was of particular interest to Prosser, who wrote a key article about it in 1939. William Prosser, *Intentional Infliction of Mental Suffering: A New Tort*, 39 MICH. L. REV. 874 (1939). In the first edition of his treatise on tort law, published in 1941, Prosser noted that "the law has been slow to accept the interest in peace of mind as entitled to independent legal protection, even against intentional invasions. It has not been until recent years that there has been any general admission that the infliction of mental distress, standing alone, may serve as the basis for an action, apart from any other tort.

Countless federal and state privacy laws have private rights of action. At the federal level, notable laws with private rights of action include the Telephone Consumer Protection Act (TCPA), the Electronic Communications Privacy Act (ECPA), the Video Privacy Protection Act (VPPA), the Fair Credit Reporting Act (FCRA), the Cable Communications Policy Act (CCPA), among others.[69] At the state level, the California Consumer Privacy Act has a private right of action, but only for data security breaches.[70] Several state unfair and deceptive acts and practices laws (called "UDAP" laws) have private rights of action.[71] The Illinois Biometric Privacy Act (BIPA) also has a private right of action.[72]

Congress has recognized statutory damages for these private rights.[73] Under the FCRA (the federal law at issue in *Spokeo*),[74] any person who willfully violates "any requirement" in the statute is liable to in an amount equal to the sum of damages sustained by the consumer *or* "damages of not less than $100 and not more than $1,000."[75] There is no harm requirement in the Wiretap Act, the Stored Communications Act, the Driver's Privacy Protection Act, the Video Privacy Protection Act, and the Cable Communications Policy Act.[76]

The Supreme Court has complicated recovery under these private rights of action by forcing plaintiffs to prove harm even though the statutes provide for statutory damages. For example, the Supreme Court has made recovery of damages under the federal Privacy Act exceedingly difficult. In *Doe v. Chao*,[77] the U.S. Department of Labor improperly disclosed the Social Security Numbers

---

[69] Telephone Consumer Protection Act (TCPA), Pub. L. No. 102-243, 47 U.S.C. § 277(c)(5); Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 18 U.S.C. §2520 (Wiretap Act), §2707 (Stored Communications Act); Video Privacy Protection Act (VPPA), Pub. L. No. 100-618, 18 U.S.C. § 2710(c); Fair Credit Reporting Act (FCRA), Pub. L. No. 90-32, 15 U.S.C. §1681n (willful violations) and §1681o (negligent violations), Cable Communications Policy Act (CCPA), Pub. L. No. 98-549, 47 U.S.C. §,551(f). For a more complete list of federal laws with private rights of action, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 160-61 (2019).

[70] California Consumer Privacy Act of 1018, AB 375.

[71] Citron, *The Privacy Policymaking of State Attorneys General*, supra note, at 798. Many UDAP laws require or have been interpreted to require a showing of injury. Almost half of state UDAP laws restrict claims for intangible injuries. *See* Carolyn Carter, *Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Law* 2, 40 (2018) https://www.nclc.org/images/pdf/udap/udap-report.pdf.

[72] Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1.

[73] The meaning of a private right of action with statutory damages is debatable. Is a private right of action a recognition of harm, with the statutory damages being imposed because harm can be difficult for plaintiffs to establish? Or is the purpose of the statutory damages to enable recovery in the absence of any harm because of other goals? Either way, the presence of statutory damages means that courts do not have to hold bench or jury trials on the question of recovery—lawmakers have supplied their judgment as to the appropriate extent of redress.

[74] 15 U.S.C. § 1681 *et seq*.

[75] 15 U.S.C. § 1681n(a).

[76] Wiretap Act, 18 U.S.C. §§ 2510-2522; Stored Communications Act, 18 U.S.C. §§ 2701-2709; Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725; Video Privacy Protection Act, 18 U.S.C. §§ 2710-2712; Cable Communications Policy Act, 47 U.S.C. §§521-573

[77] Doe v. Chao, 540 U.S. 614 (2004).

of people filing for benefits under the Black Lung Benefits Act. A group of plaintiffs sued under the Privacy Act. The lead plaintiff stated that he was "torn . . . all to pieces" by the disclosure and was "greatly concerned and worried."[78] The U.S. Supreme Court held that the statutory damages provision under the Privacy Act was only available if plaintiffs established actual damages.[79]

In a subsequent case, *Federal Aviation Administration v. Cooper*,[80] the Supreme Court held that emotional distress alone could not amount to actual damages under the Privacy Act. Three justices, writing in dissent, argued that Congress passed the Privacy Act to protect against "substantial harm" that included "embarrassment, inconvenience, or unfairness to any individual."[81] The result of the Court's holding was that a "federal agency could intentionally or willfully forgo establishing safeguards to protect against embarrassment and no successful private action could be taken against it for the harm Congress identified."[82]

The overall effect of *Doe v. Chao* and *FAA v. Cooper* has been to drastically limit the enforcement of the Privacy Act through private rights of action. Plaintiffs now have to prove willful conduct as well as establish harm, and they are forbidden from using emotional distress to do so, which is the predominant type of harm in privacy cases. Congress created the private right of action with statutory damages as an enforcement mechanism in the law, but the Court effectively cancelled it. The Privacy Act now hardly has any meaningful enforcement.

Even when federal statutes do not mention having to prove damages, some courts have taken it upon themselves to add a requirement of harm. Consider *Senne v. Village of Palatine*.[83] In that case, the U.S. Court of Appeals for the Seventh Circuit held that a plaintiff could not pursue a private cause of action for a violation of the Driver's Privacy Protection Act (DPPA) because plaintiff could not demonstrate injury. The Village of Palatine had a practice of including identifying information, such as people's height and weight, on parking tickets placed under their windshield wipers. Although the Village's practice was a clear DPPA violation, the court concluded that "we need to balance the utility (present or prospective) of the personal information on a parking ticket against the potential harm."[84] The court acknowledged that "the Act does not state that a permissible use can be offset by the danger that the use will result in a crime

[78] *Id*.
[79] Id. at 614; *see* Ryan Calo, *Privacy Harm Exceptionalism*, 12 Colo. Tech. L. J. 361 (2014) (discussing the Court's refusal to recognize emotional harm as a basis for statutory damages under Privacy Act).
[80] 132 S. Ct. 1441 (2012).
[81] *Id*. (Sotomayor, Ginsburg, and Bryer, J., dissenting) (quoting 5. U.S.C. § 552a(e)(10)).
[82] Id.
[83] Senne v. Village of Palatine, 784 F.3d.444 (7th Cir. 2015).
[84] *Id*. at 447.

or tort," yet created a harm requirement anyway.[85] The court struck down the right to sue under DPPA because plaintiff failed to provide evidence of harm, such as "stalking or any other crime (such as identity theft)," "tort (such as invasion of privacy)," disclosure over the Internet, or that "highly sensitive information" like social security number was involved.[86]

Through interpretations like these, coupled with standing, courts are undercutting the enforcement of privacy laws by creating harm requirements out of whole cloth. Courts are generally supposed to be deferential to the legislative policy goals, striking down laws only when they traduce a constitutional boundary or infringe upon a right. But courts are trading deference for activism, undermining laws in an underhanded way. Harm requirements are being invented to prevent the enforcement of privacy protections.

To sum up, courts have blocked statutory private rights of action by: (1) adding a requirement for harm via standing; (2) interpreting statutes with statutory damages in ways that require proof of harm to obtain statutory damages, thus undercutting the purpose of statutory damages provisions; (3) interpreting statutory private rights of action to require harm even when they do not have a harm requirement; and (4) adopting narrow conceptions of cognizable harm to exclude many types of harm.

The enforcement of privacy laws is a challenging issue, and unfortunately, courts are making a mess of things. Courts often lack a theory of privacy harms or any guiding principles. As Lauren Scholz observes, in many cases, the "analysis as to why a harm is not present is often superficial or absent."[87] Decisions involving harm lack a coherent vision; they are creating mischief rather than good policy.

C. HARM IN REGULATORY ENFORCEMENT ACTIONS

Regulators are often much less constrained by harm requirements. In many cases, the laws that they enforce do not require harm. The enforcement of statutes by regulators often occurs outside of the judicial system, so the issue of harm never arises.

There are circumstances where harm is a requirement for regulators to enforce, most notably Federal Trade Commission (FTC) enforcement of "unfair" acts or practices. Since the mid-1990s, the FTC has used its enforcement power under Section 5 of the FTC Act to address privacy issues.[88] Section 5 of the FTC Act

[85] *Id*.
[86] *Id*. at 448.
[87] Lauren Henry Scholz, *Privacy Remedies*, 94 Ind. L.J. 653, 662-63 (2019)
[88] *See* Marcia Hofmann, *The Federal Trade Commission's Enforcement of Privacy*, PROSKAUER ON PRIVACY (2012).

prohibits "unfair or deceptive acts or practices in or affecting commerce."[89] A "deceptive" act or practice is a "material representation, omission or practices that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment."[90] There is no mention of harm in this definition, though it does indicate that the deception must be to the "detriment" of the consumer.

The definition of unfairness is much more directly focused on harm. An "unfair" act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[91] This definition explicitly includes "likely" harm. The FTC recognizes traditional harms (and risks of such harms) such as economic and physical harms, but "more subjective types of harm" such as emotional harm are usually not considered substantial for unfairness purposes.[92] On the other hand, the FTC is able to focus on harm to consumers generally, which allows it to look to harm in a broader manner than most tort and contracts cases, which involve specific individuals.

Although regulators are able to enforce less constrained by harm, they are often limited in resources and must be highly selective about the matters they enforce.[93] State attorneys general vary considerably on how actively they enforce; some are aggressive whereas others have not brought any enforcement actions under many privacy laws that they are authorized to enforce.[94]

Because of these limitations, many privacy laws rely upon private litigation to enforce the law. The Telephone Consumer Protection Act (TCPA) is a prime example of this type of enforcement mechanism. The law restricts unsolicited commercial telemarketing calls, robocalls, and faxes, and it is enforced by the Federal Communications Commission (FCC) and state attorneys general. To augment this enforcement, the law includes a private right of action with statutory damages of $500 for each violation and $1500 for each knowing or willful violation.[95] Because the TCPA enforcement process is tedious and time-

---

[89] 15 U.S.C. § 45.

[90] 15 U.S.C. § 45(n); *See* Federal Trade Commission, Policy Statement on Deception (1983), appended to In re Cliffdale Assoc., 103 F.T.C. 110, 174 (1984), http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[91] 15 U.S.C. § 45(n); Federal Trade Commission, Policy Statement on Unfairness (1980), Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[92] *Federal Trade Commission, Policy Statement on Unfairness* (1980), Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm; Marcia Hofmann, *The Federal Trade Commission's Enforcement of Privacy*, PROSKAUER ON PRIVACY, at 2.

[93] Citron, *State Attorneys General, supra* note X, at 799.

[94] *Id.* at 755 ("In the past fifteen years, a core group of states have taken the lead on privacy enforcement: California, Connecticut, Illinois, Indiana, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Texas, Vermont, and Washington.").

[95] 47 U.S.C. §227(c)(5).

consuming and because many TCPA cases involve small matters that do not make splashy headlines, FCC enforcement has been modest.[96] In one year, for example, there were 47,704 complains but the FCC only issued 23 citations.[97] In practice, private litigation has become the primary source of TCPA enforcement.[98]

Litigation by private parties thus supplements enforcement by regulatory agencies and state attorneys general, and in a number of instances, private litigation serves as the primary enforcement mechanism of a law. Based on this enforcement role, private parties enforcing a law through private litigation are often referred to as "private attorneys general."[99] As one court aptly explained, the "award of statutory damages could also be thought a form of bounty system, and Congress is permitted to create legally enforceable bounty systems for assistance in enforcing federal laws, provided the bounty is a reward for redressing an injury of some sort (though not necessarily an injury to the bounty hunter)."[100] And, these cases typically require a showing a harm, which is often the death knell if plaintiffs cannot show financial or physical harm.

II. A TYPOLOGY OF PRIVACY HARMS

Privacy harms have been a challenge to conceptualize because they are so varied. Privacy is an umbrella concept that encompasses different yet related things.[101] It is no surprise that privacy harms involve different yet related concerns. Privacy harms not only differ in type but also in their severity.

In this Part, we discuss the various types of privacy harms and whether the law currently recognizes them.[102] For many types of privacy harm, the law lacks clarity and consistency as to whether the harm is cognizable. We contend that in most cases, these distinct types of harms should be treated as cognizable harms. For several of these types of harms, there is support in caselaw and doctrines in other contexts to support recognition of cognizable harm.

---

[96] Spencer Weber Waller, Daniel B. Heidtke, and Jessica Stewart, *The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology*, 26 Loyola Consumer L. Rev. 343, 376-78 (2014)

[97] *Id.* at 378.

[98] *Id.* at 376 ("Private parties have largely been responsible for enforcement of the TCPA.").

[99] William B. Rubenstein, *On What A "Private Attorney General" Is--And Why It Matters*, 57 Vand. L. Rev. 2129 (2004).

[100] Crabill v. Trans Union, LLC, 259 F.3d 662, 665 (7th Cir. 2001).

[101] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

[102] The typology of privacy harms differs from the taxonomy of privacy problems that one of us has developed. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008). The taxonomy concerns the concept of privacy, which involves attempts to deal with a set of related problems. Many of the problems in the taxonomy can create the same type of privacy harm.

A. PHYSICAL HARMS

Privacy violations can create physical harms, which are well-recognized as cognizable under the law. Indeed, setbacks to physical health, where clear and obvious, have rarely been disputed as cognizable harms.

The improper sharing of personal data can create unique opportunities for physical violence. Rebecca Schaeffer, a model and actress, was murdered after a stalker obtained her home address with the help of a private investigator who obtained it from California motor vehicles records. The Internet has made it even easier for such sharing of personal data to lead to physical assault. In December 2009, an online advertisement on Craigslist featured a woman's photograph next to her "interest" in "a real aggressive man with no concern for women." The woman's ex-boyfriend Jebidiah Stipe wrote the post.[103] More than 160 people responded to the ad, including Ty McDowell.[104] Stipe sent McDowell text messages with the woman's home address and false claims of her fantasies about "humiliation, physical abuse, and sexual abuse." McDowell attacked the woman as she returned home, forcing his way inside. At knifepoint, he raped her and abused her with a knife sharpener.[105] When caught by the police, McDowell said that the woman had asked him to rape her.[106]

Entities handling personal data have been found liable for negligently, knowingly, or purposefully paving the way for a third party to physically injure someone. In *Remsburg v. Docusearch, Inc.*,[107] a disturbed man named Liam Youens purchased personal data about Amy Boyer from data broker Docusearch.[108] To satisfy Youens's request for the address of Boyer's employer, Docusearch hired a person to find out by calling Boyer, lying to her about the reason for the call and inducing her to reveal the address.[109] Docusearch gave the address to Youens who then confronted Boyer at work and killed her.[110]

The New Hampshire Supreme Court found that the broker had a duty to exercise

---

[103] Brian, "Craigslist Rapists Get 60 to Life: Ad Seeking Someone with 'No Regard' for Women Led to Rape," Victimized over the AOC (blog), July 3, 2010, http://victimsover18.blogspot.com/2010/07/craigslist-rapists-get-60-to-life-ad.html.

[104] William Browning, "Wyo. Craigslist Rape Victim Speaks for the First Time," *AP Alert,* September 24, 2010.

[105] William Browning, "Details Emerge in Web Rape Case," *Star-Tribune* (WY), February 5, 2010, http://trib.com/news/local/article_edb73077-0bbc-5bc2-b9ea-b3fe5c9aedce.html; Pete Kotz, "Jebidiah Stipe Used Craigslist Rape Fantasy Ad to Get Revenge on Ex Girlfriend," True Crime Report (blog), February 9, 2010 (11:13 A.M.), http://www.truecrimereport.com/2010/02/jebidiah_stipe_used_craigslist.php.

[106] DeeDee Correll, "Craigslist Implicated in Rape Case: A Wyoming Man Is Accused of Using the Website to Engineer an Ex-Girlfriend's Assault," *Los Angeles Times,* January 11, 2010, A9.

[107] 816 A.2d 1001 (N.H. 2003).

[108] *Id.* at 1005-06.

[109] *Id.*

[110] *Id.*

reasonable care in releasing information to a third party due to the foreseeable risk of criminal conduct. A private investigator "owes a duty to exercise reasonable care not to subject a third person to an unreasonable risk of harm."[111] For the court, the risk of criminal misconduct was sufficiently foreseeable so that an "investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client." According to the court, information brokers should know that stalkers often use their services to obtain personal data about victims.

Privacy claims involving the negligent enablement of physical injuries can be traced to premises liability cases. In *Kline v. 1500 Massachusetts Avenue Apartment Corp.*,[112] the plaintiff was attacked and robbed in the hallway just outside her apartment. The landlord left the building unguarded even though tenants had been assaulted and robbed in the building's common areas.[113] The court held that residential apartment owners had a duty to exercise reasonable care to protect tenants from third party violence.[114] The landlord was in a better position than the tenant to adopt precautionary measures and better situated than the police to diminish the risk of criminal assault on its premises.[115]

Although courts clearly recognize harm from physical injuries, courts are reluctant to hold online service providers responsible when their activities promote, facilitate, or enable such harm. The physical harm facilitated via online stalking is akin to the physical injuries that result when landlords fail to secure their property. In cases involving owners of residential property, hospitals, day care centers, and shopping malls, courts have extended liability to the owners for a third party's criminal acts [116] Similar to these owners, online platforms and service providers exercise control over the use and security of their services, courts treat them differently.[117] Due in part to Section 230 of the Communications Decency Act and the legal shield it provides, courts have not taken up the invitation to treat digital spaces with the same set of rules as with physical places.[118]

---

[111] *Id.*

[112] 439 F.2d 477 (D.C. Cir. 1970).

[113] *Id.* at 479.

[114] *Id.* at 487.

[115] *Id.* at 480.

[116] Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L.J. 1553, 1582 (2005).

[117] See Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 Cal. L. Rev. 1819 (2010).

[118] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Danielle Keats Citron, *Cyber Mobs, Disinformation, and Death Videos: The Internet As It Is (and As it Should Be)*, 118 Mich. L. Rev. 1073 (2020); Danielle Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 Fordham L. Rev. 401 (2017).

B. ECONOMIC HARMS

Privacy violations can result in financial losses that the law has long understood as cognizable harm. Even small economic harms are deemed cognizable by courts.[119] In cases involving identity theft, plaintiffs can prove harm when identity thieves steal their personal data and use it to conduct fraudulent transactions in their names.[120] Difficulties arise if plaintiffs are eventually able to clear up the financial pollution left by identity thieves. Suppose an identity thief takes out a credit card in a victim's name. The victim spends a considerable amount of time clearing up the mess and establishing that the debt is not the victim's responsibility. Victims might argue that their time, stress, and anxiety to mitigate future economic harm should be compensated, but courts often look askance as these things as bases for cognizable harm.[121] Many cases involving economic harm are data breach cases. As we noted in our article on data breach harms, plaintiffs have difficulty providing a causal link between particular data breaches and identity theft.[122] Moreover, in many cases, the identity theft has not yet occurred, and many courts refuse to recognize a harm for the risk of future economic loss.[123]

In cases involving the use and sharing of personal data, courts often refuse to find economic harm. In *Dwyer v. American Express*,[124] a group of cardholders sued American Express for creating profiles of them based on their spending habits and using these profiles for marketing. The cardholders argued that this activity was a violation of the tort of appropriation of name or likeness. They contended that American Express appropriated for its own use or benefit their names or likenesses without their consent. The court, however, concluded that although "each cardholder's name is valuable to defendants," the value of the American Express lists was due to its "categorizing and aggregating these names." American Express's use of the information does "not deprive any of the cardholders of any value their individual names may possess."[125] Thus, the cardholders could not establish harm.

Many privacy violations involve the loss of important opportunities rather than direct financial injuries. We could not find any privacy cases recognizing a harm for loss of productivity or time to deal with privacy violations. In other contexts, however, courts readily recognize a similar type of harm. For example, courts recognize loss of consortium, which is defined as the "conjugal fellowship of husband and wife, and the right of each to the company, cooperation, affection,

---

[119] LaVigne v. First Cmty. Bancshares, Inc., 215 F. Supp. 3d 1138, 1146 (D.N.M. 2016) ("Regardless of how small the harm is, it is actual and it is real.").
[120] Solove & Citron, *Risk and Anxiety, supra* note X at 754-56.
[121] *Id.* at 748-53.
[122] *Id.* at 756-60.
[123] *Id.* at 750-52.
[124] 652 N.E.2d 1351 (Ill. App. 1995).
[125] For a different outcome in an action brought by New York Attorney General under state UPDA law, see Citron, *supra* note.

and aid of the other in every conjugal relation."[126] The concept of "consortium" translates the loss of quality time into an economic harm. Although this concept has firm roots in the law, it has not developed to encompass the loss of quality time more generally and has not become part of privacy cases.

C. REPUTATIONAL HARMS

Privacy violations can result in reputational injuries, which have a long history of recognition. Reputational harms impair a person's ability to maintain "personal esteem in the eyes of others" and can taint a person's image.[127] They can result in lost business, employment, or social rejection.

The law has treated reputational harms as distinct from physical and property injuries. As Justice Potter Stewart remarked of defamation law, an individual's right to the protection of his good name reflects "our basic concept of the essential dignity and worth of every human being."[128] Under the umbrella of defamation law, the torts of libel and slander impose liability when a person makes a "false and defamatory statement concerning another."[129] The tort of false light, which emerged out of the Warren and Brandeis article, protects against widely publicizing "a matter concerning another that places the other before the public in a false light" that is "highly offensive to a reasonable person."[130]

A longstanding rule in defamation law is that certain defamatory falsehoods (such as the claim that someone has a sexually transmitted disease) warrant the recovery of damages without evidentiary proof.[131] Although presumed damages have been disallowed for defamation lawsuits by public officials and public figures, such damages are permitted in a "vast number of cases."[132] Additionally, in other cases where plaintiffs must prove reputational damage but cannot do so, they still may obtain "nominal damages" – typically one dollar.[133] Although common in defamation cases, nominal damages are not restricted to defamation.[134] As Megan Cambre notes, "An award of nominal damages recognizes that a plaintiff's right has been violated. It further provides recovery for that legal wrong."[135] There is currently a circuit split on whether nominal

---

[126] BLACK'S LAW DICTIONARY

[127] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 175 (2008).

[128] Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) (Stewart, J., concurring).

[129] Restatement (Second) of Torts § 559.

[130] Restatement (Second) of Torts § 652E.

[131] Michael K. Steenson, *Presumed Damages in Defamation Law*, 40 Wm. Mitchell L. Rev. 1492, 1492 (2014).

[132] *Id.*

[133] Megan E. Cambre, *A Single Symbolic Dollar: How Nominal Damages Can Keep Lawsuits Alive*, 52 Ga. L. Rev. 933, 937 (2018).

[134] *Id.* at 938 ("Nominal damages are available as a remedy in all types of cases.").

[135] *Id.* at 950.

damages are sufficient to confer standing.[136]

In at least one case, a court recognized reputational harm caused indirectly when personal data was misused by a social media platform to grow membership in the platform's user base. In *Perkins v. LinkedIn*, the professional social network site downloaded users' email contacts, using them to ask users' contacts to connect on the site without the users' permission. Users sued LinkedIn on the grounds that sending repeated invitations to their contacts caused them reputational harm because their contacts might think that they sent the repeated invitations. The court concluded that they had alleged cognizable harm – that LinkedIn engaged in misleading commercial speech causing injury.[137]

D. EMOTIONAL HARMS

One of the most common types of harm caused by privacy violations is emotional distress. Emotional distress encompasses a wide range of emotions, including annoyance, frustration, anger, and various degrees of anxiety.

The impact of emotional harm varies depending upon the emotion triggered. Fear can be among the most damaging emotions given its impact on people's life choices. One of us has chronicled the devastating impact that fear has had on women who faced a perfect storm of impersonation, doxing, nude photos, and threats online.[138] Privacy violations can cause emotional distress that can impede someone's life as much as certain physical injuries. The emotional toll of identity theft can adversely affect victims' work and relationships.[139]

Courts, however, have struggled with how to recognize emotional distress as a cognizable harm, resulting in a messy and inconsistent body of caselaw. In one sphere of tort law—the privacy torts spawned from Warren and Brandeis's article—courts have consistently recognized emotional distress alone as cognizable harm. The privacy torts, however, are more of an exception than the rule. The special oasis afforded to the privacy torts likely is due to their genesis from the Warren and Brandeis article, which emphatically noted that privacy violations primarily involve an "injury to the feelings."[140] Privacy invasions interfered with a person's "estimate of himself," inflicting "mental pain and distress, far greater than could be inflicted by mere bodily injury."[141]

Specifically addressing judicial reluctance to recognizing emotional harm, Warren and Brandeis began by noting how the common law had matured to

---

[136] *Id.* at 948-50.
[137] Perkins v. LinkedIn, 53 F. Supp. 3d 1222 (N.D. Cal. 2014).
[138] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Danielle Keats Citron, *Cyber Civil Rights*, 89 BU Law Rev. 61 (2009).
[139] Bureau of Justice Statistics, "Victims of Identity Theft, 2012," December 2013, at 10 http://www.bjs.gov/content/pub/pdf/vit12.pdf.
[140] *Id.* at 197.
[141] *Id.*

recognize and redress a variety of types of intangible harms beyond physical ones. "[I]n early times," they wrote, "the law gave a remedy only for physical interference with life and property."[142] Subsequently, the law expanded to recognize incorporeal injuries; "[f]rom the action of battery grew that of assault. Much later there came a qualified protection of the individual against offensive noises and odors, against dust and smoke, and excessive vibration. The law of nuisance was developed."[143] They noted how defamation law protected a person's name without requiring proof of financial or physical harm.[144] In essence, Warren and Brandeis argued that recognition of emotional harm was a sign of a more advanced civilization, and by implication, failure to do so would be crude and uncivilized. Because Warren and Brandeis tied the privacy torts so tightly to emotional harm, it would be somewhat odd and nonsensical for courts to recognize the privacy torts but not allow pure emotional harms for recovery.

Privacy tort cases readily allow emotional distress as the sole basis of harm.[145] Cases "collectively reject any suggestion that special damages or physical injuries are a threshold pre-condition to recovery."[146] Courts have recognized as cognizable harms feelings of violation, mortification, fear, humiliation, and embarrassment, among other things.[147] The Restatement of Torts clearly indicates that plaintiffs can recover for emotional distress alone.[148]

In countless privacy tort cases, courts do not question the viability of the harm.[149] The issue is so clear and settled that courts do not even bother to mention it. Oddly, beyond the four privacy torts, courts view pure emotional distress with skepticism. Perhaps this odd disjunction is due to judges being relatively unfamiliar with the Warren and Brandeis privacy torts, and thus they lack an appreciation of the clear recognition of emotional distress in these cases.

In contract law, courts have been reluctant to recognize emotional harm, but they have shifted on this issue to move toward a greater allowance of recovery for emotional harm. The general rule is that emotional distress damages are not permitted for breach of contract. The rule emerges from the famous English case from 1854, *Hadley v. Baxendale*.[150] Although *Hadley* is the prevailing rule, it was once considered a radical departure from the existing rule that damages for breach of contract could encompass all losses suffered by the plaintiff, including emotional distress. *Hadley* was part of a general movement in England to limit

---

[142] *Id.* at 193.
[143] *Id.* at 194.
[144] Restatement (Second) of Torts § 623 (1977). Defamation liability includes redress for emotional distress caused by the defamatory publication. *Id.*
[145] Brents v. Morgan, 299 SW 967, 971 (Ky 1927).
[146] DAVID. A. ELDER, PRIVACY TORTS §3-8 at p. 3-89.
[147] ELDER 3:8 3-90 to 3-92.
[148] Restatement (Second) of Torts 652H comm. b.
[149] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety, supra,* at X.
[150] Hadley v. Baxendale, 156 Eng. Rep. 145 (1854).

the discretion of juries and to shift more power to judges.[151] Justifications for the *Hadley* rule in U.S. contract law are based on fears of fabricated claims, disproportionate compensation, and unforeseeable damages.[152]

Nonetheless, courts have been making a number of exceptions to the *Hadley* rule, such as "when the breach is willful or wanton in nature of if the breach causes bodily harm."[153] Another exception is when the "contract is personal in nature," such as contracts to take photographs, to supply wedding dresses, or to perform cosmetic surgery.[154] As one commentator has noted, "courts have frequently allowed non-economic damages in breach of contract actions, despite forging the limiting rule, and clearly 'have not applied it inflexibly.'"[155] Although the law of recovery of emotional distress damages from contracts is in flux and does not clearly encompass privacy and security issues, there is enough of a foundation in the law for courts to at least explore the issue as law develops.

E. RELATIONSHIP HARMS

Privacy violations can harm personal and professional relationships as well as relationships with organizations. People modulate personal relationships by maintaining boundaries around their information or by withholding information from some people and not others. Strangers develop close relationships by entrusting each other with deeply personal information. Consider communications among people using fertility tracking apps. On apps like Clue, subscribers gather online to explore struggles with miscarriages, abortions, and infertility. They often form bonds with each other. Their relationships depend upon trusting each other to maintain the confidentiality of their information.

Relationship harms are two-fold: most immediately, the loss of confidentiality and in the longer term, damage to the trust that is essential for the relationship to continue.[156] As Nancy Levit remarks, the "development of protection for relational interests evidences a communitarian view of the role of tort law. . . . The vision being promoted is one of the responsible social interaction: a commitment to the value of the permanency of relationships and to appropriate treatment within those relationships."[157]

---

[151] Mara Kent, *The Common-Law History of Non-Economic Damages in Breach of Contract Actions Versus Willful Breach of Contract Actions*, 11 Tex. Wesleyan L. Rev. 481, 487-91 (2005).
[152] Kent, Common-Law History, supra at 493.
[153] Kent, *supra*, at 493. *See also* 11 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 59.1, at 539 (Joseph M. Perillo ed., rev. ed. 2005) (exceptions to *Hadley* rule include "(1) cases where such suffering accompanies a bodily injury; and (2) where it was caused intentionally or in a manner that is wanton or reckless").
[154] Kent, *supra*, at 501.
[155] Kent, *supra*, at 493 (quoting E. ALLAN FARNSWORTH, CONTRACTS § 12.17 (3d ed. 1999)).
[156] See Danielle Keats Citron, W*hy Sexual Privacy Matters for Trust*, 96 Wash. U. L. Rev. 1189 (2019).
[157] Levit, *supra* note.

The law has recognized relationship harms, though it has done so inconsistently. Evidentiary privileges restrict the disclosure of communications between attorney and client, priest and penitent, husband and wife, and psychotherapist and patient.[158] The point of protecting certain relationships is to foster candid expression and the preservation of the relationships.

The breach of confidentiality tort extends to certain relationships—mostly professional ones—but it fails to protect many other relationships, such as personal and familial ones.[159] Courts have refused to treat companies as having a duty to keep personal data confidential even though they are in a position of trust and exercise power over individuals' personal data.[160]

The law of fiduciary relationships also safeguards against relationship harms. A fiduciary relationship has long been part of the law of trusts and has been recognized as a special relationship.[161] Because the trustee is in a "position of special trust, the trustee owes certain special duties to the beneficiary."[162] As one of us has noted, a wide array of relationships have been deemed to be fiduciary ones, and the law is open-ended about recognizing such relationships.[163] According to Jack Balkin, "Because of their special power over others and their special relationships to others, information fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[164] Fiduciaries owe special duties including confidentiality, loyalty, transparency, care, and others.[165]

The relationships recognized as fiduciary ones is open-ended rather than a fixed list. In breach of confidentiality cases, courts have recognized fiduciary relationships between doctor and patient, lawyer and client, bank and customer, as well as school and student.[166] One of us argued that the concept of fiduciary relationships can be expanded to regulate consumer privacy because "companies collecting and using our personal information stand in a fiduciary relationship with us."[167]

---

[158] SOLOVE & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note _, at 499-504.
[159] Solove & Richards, *Privacy's Other Path, supra* note, at 176-78.
[160] *Id.* at 157-58.
[161] ARI WALDMAN, PRIVACY AS TRUST (2019); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law* (on file with authors); Neil M. Richards & Woodrow Hartzog, *Privacy Law's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687 (2020).
[162] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102 (2004).
[163] *Id.* at 103.
[164] Jack Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1186 (2016).
[165] Lauren Henry Scholz, *Fiduciary Boilerplate*, __ J. Corp. L. __ (draft at p. 65) (June 5, 2020), available at https://ssrn.com/abstract=3620164.
[166] *Id.*
[167] *Id.* at 103.

Recently, a number of scholars have further developed this argument, most notably Jack Balkin, Woodrow Hartzog, Neil Richards, and Lauren Scholz. As Lauren Scholz observes, "[f]iduciary law's core goal of preventing opportunistic behavior."[168] She contends that "[i]mplying a fiduciary relationship has the advantage of enabling courts and the justice system to allow and enforce expectations as they are situated in concrete relationships."[169] Thus far, however, the application of the law of fiduciary relationships to privacy has developed slowly, mainly in breach of confidentiality cases in a limited set of professional relationships, but it certainly has potential to develop further in the future.

F. CHILLING EFFECT HARMS

Privacy violations can produce harm by inhibiting people from engaging in certain civil liberties such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas. Such harm is often called a "chilling effect."[170] As Frederick Schauer observes: "The very essence of a chilling effect is an act of deterrence."[171] According to Neil Richards, the failure to protect privacy can chill individuals from engaging in reading or researching.[172] In cases involving rights under the First Amendment to the U.S. Constitution, courts have sometimes recognized harm when people are chilled from exercising rights, such as free speech or free association.[173]

Chilling effects have an impact on individual speakers and society at large as they reduce the range of viewpoints expressed and the nature of expression that is shared.[174] Monitoring of communications can make people less likely to engage in certain conversations, express certain views, or share personal information. Consider the impact of news that the gay dating app Grindr had shared subscribers' HIV status with analytics firms. Subscribers expressed profound dismay. Individuals told the press that they would no longer share that information on that app or any dating app—it was simply not worth the possibility that employers or others could find out their HIV status and hold it against them.[175]

Courts have been uneasy about recognizing chilling effects, and the law has

---

[168] *Id.* at 66.
[169] *Id.* at 67.
[170] Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 NYU L. Rev. 112, 142-43 (2007).
[171] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 701 (1978).
[172] NEIL M. RICHARDS, INTELLECTUAL PRIVACY 165 (2014).
[173] Solove, *First Amendment as Criminal Procedure, supra* note X, at 143-51.
[174] NEIL M. RICHARDS: INTELLECTUAL PRIVACY (2014); Neil M. Richards, *Intellectual Privacy*, Tex. L. Rev.; Julie E. Cohen, *Subject as Object*, Stan. L. Rev.
[175] Danielle Keats Citron, *A New Compact for Sexual Privacy*, William & Mary L. Rev. (forthcoming).

wavered. In *Laird v. Tatum*, the U.S. Supreme Court limited the chilling effect doctrine by concluding that "[a]llegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[176] Courts have subsequently struggled to determine the line between an objective and subjective chill.[177]

Despite the somewhat murky status of the law, the concept of chilling is widely accepted even if its precise contours remain unclear. Although the chilling effect doctrine emerges from cases involving the First Amendment to the U.S. Constitution, the concept could certainly be applied to other legal contexts.

G. DISCRIMINATION HARMS

Privacy violations can cause discrimination harms, which involve entrenching inequality and disadvantaging women and people from marginalized communities. Discrimination harms thwart people's ability to have an equal chance to obtain and keep jobs, secure affordable insurance, find housing, and to pursue other crucial life opportunities. The misuse of personal data can be particularly costly to women, sexual minorities, and nonwhites given the prevalence of destructive stereotypes and the disproportionate surveillance of women and marginalized communities in their intimate lives.[178] For example, employers and health insurance companies can access information that women share with period-tracking apps (including their moodiness and cramps), which could result in raised premiums and denied promotions.[179] Women and minorities are often disproportionately targeted for vicious online harassment, which often involves doxing – the sharing of their personal data such as home address and location – in order to expose them to physical danger.[180] Harassers post victims' nude photos and embarrassing information about their sex lives or sexual health, causing them substantial emotional and reputational harm.[181] Although these types of harm are separate categories in our typology, there is a distinct and additional dimension that they add: the entrenchment of existing patterns of inequality.

In cases involving cyber mobs that inundate victims with crude, threatening, and

[176] Laird v. Tatum, 408 U.S. 1 (1972).
[177] Solove, *First Amendment as Criminal Procedure*, *supra* note X, at 143-44.
[178] Danielle Keats Citron, *A New Compact for Sexual Privacy*, William & Mary L. Rev. (forthcoming). One of us (Citron) has explored the integral connection between privacy violations and discrimination throughout her scholarship. See, e.g., DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Danielle Keats Citron, *Sexual Privacy*, Yale L.J. (2019); Danielle Keats Citron, *Spying Inc*., 72 Wash. & Lee L. Rev. 1243 (2015); Citron, *Cyber Civil Rights*, supra note. That work has been inspired by and built on the pathbreaking insights of privacy scholar Anita Allen. See, e.g., Anita Allen, Unpopular Privacy: What We Must Hide (2012); Uneasy Access: Privacy for Women in a Free Society (1988).
[179] Drew Harwell, *Is Your Period App Sharing Your Intimate Data with Your Boss*?, Washington Post (April 10, 2019).
[180] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note.
[181] *Id.*; Citron, *Sexual Privacy*, *supra* note.

abusive comments, plaintiffs have sought to protect themselves by bringing privacy tort cases.[182] But litigation has complicated by the fact that the harm is often caused by the totality of the comments, making it hard to allocate the harm among the multitude of commenters.[183] The members of the mob are often anonymous, and it is difficult and expensive to identify them.[184] Even when the perpetrators are tracked down, suing them is often impractical because they often are unable to pay enough monetary damages to incentivize lawyers to litigate.[185] To combat cyber mobs effectively, victims turn to social media platforms to shut down the mob, but Section 230 of the Communications Decency Act immunizes these platforms from liability for user-generated content.[186]

In some cases, the information about plaintiffs is innocuous in the abstract, such as their home addresses. Such information may already be available online from other sources. But when this data is used to dox victims, the data no longer is innocuous. Courts are generally reluctant to view the disclosure of home addresses as harmful (or even as a violation of privacy) unless plaintiffs have done everything that they can to keep their home addresses from the public (such as removing their addresses from the white pages), but some courts have recognized the harm.[187] For example, in *Planned Parenthood v. American Coalition of Life Activists*, an anti-abortion activist group doxed abortion doctors. Some of these doctors were murdered, and the living ones whose personal information was posted online sued and argued that they feared for their safety. The court sided with the doctors.[188] Cases like *Planned Parenthood* are rare, however, and few plaintiffs have been able to use litigation to combat doxing.

Beyond doxing and threats targeted at people in marginalized groups, there are less overt forms of discrimination harms. These harms are difficult to redress because they often occur in the shadows. The decision-making process of employers, insurance companies, landlords, and other powerful actors is opaque. If an employer used a third-party hiring service to score candidates, then rejected applicants will have no way to know that the hiring service relied upon their intimate information (like their painful periods or infertility).[189]

---

[182] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note, at 133; Citron, *Sexual Privacy*, supra note.

[183] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note.

[184] Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2018).

[185] CITRON, HATE CRIMES IN CYBERSPACE, *supra* note.

[186] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007); DANIELLE CITRON, HATE CRIMES IN CYBERSPACE (2014); Danielle Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61 (2009).

[187] *See, e.g.*, Benz v. Washington Newspaper Publishing Co., 2006 WL 2844896 (D.D.C. Sept. 29, 2006) (refusing to dismiss plaintiff's public disclosure claim stemming from defendant's publication of her home address online next to the suggestion that she was interested in sex because her home address was not listed in the phone book).

[188] Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058, 1065 (9th Cir. 2002) (en banc).

[189] Citron, *A New Compact for Sexual Privacy*, *supra* note, at. There is a wealth of scholarship

A key aspect of discrimination harms is the unequal frequency, extensiveness, and impact of privacy violations on marginalized people. People of color are disproportionately targeted by surveillance.[190] Algorithms that appear neutral often have disproportionate effects on minorities.[191] Poor people are often subjected to oppressive surveillance as part of public assistance bureaucracy. Black mothers are "stripped of formal privacy rights claims by signing an encompassing waiver" when applying for assistance.[192] As Khiara Bridges contends, "poor mothers are not given privacy rights because society, and thus the law, presumes that their enjoyment of privacy will realize no value or negative value."[193] Mary Anne Franks notes that surveillance often does not affect marginalized and non-marginalized people equally: "For the less privileged members of society, surveillance does not simply mean inhibited Internet searches or decreased willingness to make online purchases; it can mean an entire existence under scrutiny, with every personal choice carrying a risk of bodily harm."[194]

Privacy torts and other tort claims lack the language and concepts to address discrimination harms.[195] The disparate effects of certain privacy violations are not considered as part of the harm equation. In contrast, federal statutes do recognize privacy violations as producing discrimination harm, such as the federal Genetic Information Nondiscrimination Act (GINA) and the Americans with Disabilities Act (ADA). GINA prohibits employers from requesting, requiring, or obtaining employees' genetic information. The ADA limits the ability of employers to make medical examinations or inquiries of job applicants under a number of circumstances.[196]

The civil rights legal tradition has the capacity and vocabulary to address discrimination harm—the denial of social and economic opportunities due to one's membership in a protected group.[197] Federal and state civil rights laws secure the ability to work, attend school, use the telephone, secure housing, and

---

and research exploring the discriminatory impacts of algorithmic decision-making in the commercial sector. See, e.g., I. Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Conference on Artificial Intelligence, Ethics, and Society (2019); J. Dastin, Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women, Reuters.

[190] Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N. Mexico L. Rev. 301 (2020).

[191] ANDREW GUNTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 47 (2017).

[192] JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 71 (2001).

[193] KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 12 (2017); Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, B.U. L. Rev. (2018).

[194] Mary Anne Franks, *Democratic Surveillance*, 30 Har. J. L. & Tech. 426 (2017); *see also* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (2000).

[195] Citron, *A New Compact for Sexual Privacy*, *supra* note.

[196] 42 U.S.C. §12112(d).

[197] Title VII; FMLA; Title IX; Americans with Disabilities Act.

vote on equal terms.[198] But these laws still have not been applied sufficiently to privacy violations. One of us has proposed situating and treating privacy as a civil right so discrimination harms caused by privacy violations can be addressed.[199] Existing civil rights laws admittedly do not cover all social goods in need of protection[200] or to all parties given the state action doctrine.[201] They mostly do not constrain corporate handling of personal data.[202] Nonetheless, situating private sector surveillance of intimate life as a matter of civil rights helps begin the conversation about what those freedoms *should* be in the context of privacy law specifically and civil rights law more generally.

H. THWARTED EXPECTATIONS HARMS

A common type of privacy violation involves thwarting people's privacy expectations by breaking promises made about the collection, use, and disclosure of personal data. Courts are generally dismissive of thwarted expectations as a cognizable harm unless it is accompanied by other harms, such as reputational, economic, or emotional harm. As Margot Kaminsky aptly observes, "in the information privacy context, the Supreme Court and others have repeatedly asked for privacy plaintiffs to show something more."[203]

When data is used improperly without people's consent, courts tend to look for economic harm rather than recognize that improper use of personal data is harmful in and of itself. In *In re Google, Inc. Privacy Policy Litigation*[204] plaintiffs sued Google for using their personal data in different ways than had been promised, but the court found that they lacked standing because they failed to allege how Google's "use of the information deprived them of the information's economic value."[205] In *Fraley v. Facebook*, the court also focused on economic value when it concluded that plaintiffs suffered harm when

---

[198] Danielle Citron & Mary Anne Franks, *Cyber Civil Rights in an Age of COVID*, HARV. L. REV. BLOG (May 14, 2020), https://blog.harvardlawreview.org/cyber-civil-rights-in-the-time-of-covid-19/.

[199] Danielle K. Citron, *Why We Need to Talk About Privacy as a Civil Right*, ILLINOIS L. REV. (forthcoming in symposium issue on Helen Norton's When Government Speaks); Citron, *Cyber Civil Rights, supra* note, at 89 ("Traditional tort and criminal law fail to respond to such systemic harm and, indeed, may obscure a full view of the damage.").

[200] In her important new book, Robin West calls for a transformative understanding of civil rights that does not merely prohibit discrimination but that entails rights essential to the justice of the nation. ROBIN L. WEST, CIVIL RIGHTS: RETHINKING THEIR NATURAL FOUNDATION (2019).

[201] *Id*. (exploring the various ways that civil rights laws have failed to fulfill their potential to protect social goods themselves).

[202] As scholars have explored, antidiscrimination laws like Title VII are ill-suited to address the use of discriminatory algorithms in employment matters. See Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811 (2020); Pauline Kim, *Data Discrimination at Work*, 58 WILLIAM & MARY L. REV. 857 (2018); Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

[203] Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DePaul L. Rev. 413, 416 (2017).

[204] 2013 WL 6248499 (N.D. Cal. 2013).

[205] Id.

Facebook used their "likes" to promote products without their permission. [206] The court held that "personalized endorsement" to friends "has concrete, provable value in the economy at large."[207]

Generally, courts have not found harm when companies share personal data with third parties in violation of their privacy policies. In *Smith v. Chase Manhattan Bank*, for example, the court concluded that plaintiffs suffered no harm when a bank that sold their personal data to third parties in violation of its privacy policy: "[C]lass members were merely offered products and services which they were free to decline. This does not qualify as actual harm."[208]

Plaintiffs have fared better when statutes are the source of the expectation that data will not be shared. In *In re Nickelodeon Consumer Privacy Litigation*, the court concluded that a Viacom's improper collection of personal data about the videos people watched on its website and its disclosure of the data to Google was a cognizable harm. The court noted that "when it comes to laws that protect privacy, a focus on economic loss is misplaced" and that "the unlawful disclosure of legally protected information" was "a clear de facto injury."[209] In *Eichenberger v. ESPN, Inc.*, the Ninth Circuit concluded that sharing personal data with a third party in violation of the Video Privacy Protection Act (VPPA) was a harm because "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."[210]

In contract law, courts are adamant about focusing on economic harm. In *In Re Google, Inc. Cookie Placement Privacy Litigation*, Google tracked users' Internet activity in violation of its promise to respect users' "do not track" settings. The court held that the plaintiffs could not prove harm because they could not demonstrate that Google interfered with their ability to monetize their personal data.[211] In a series of cases involving airlines that shared passenger data with the government in violation of their privacy policies, courts held that the plaintiffs failed to show harm.[212] For example, in *In re Jet Blue Airways Corp. Privacy Litigation*, the court held that recovery in contract "allows only for economic losses."[213]

Many courts fixate on whether plaintiffs have read and relied on the privacy policy of a company, but the privacy policy plays a small role in forming

[206] Fraley v. Facebook, 830 F. Supp. 2d 785 (N.D. Ca. 2011).
[207] *Id.* at 799.
[208] Smith v. Chase Manhattan Bank, 293 A.D.2d 598, 599 (N.Y.App.Div. 2002).
[209] In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 272-73, 274 (3d Cir. 2016).
[210] Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017).
[211] In re Google, Inc. Cookie Placement Privacy Litig., (D. Del. Oct. 9, 2013).
[212] In re Jet Blue Airways Corp. Privacy Litigation, 379 F. Supp.2d 299, 326 (E.D.N.Y. 2005); In re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Mill. 2004); Dyer v. Northwest Airlines Corp., 334 F.Supp.2d 1196 (D.N.D. 2004).
[213] In re Jet Blue Airways Corp. Privacy Litigation, 379 F. Supp.2d 299, 326 (E.D.N.Y. 2005).

people's privacy expectations.[214] This is especially true because hardly anyone reads privacy policies, and it is not rational to do so given the vast number of organizations collecting data about people.[215] Instead of focusing on the promises in privacy policies in isolation, courts should consider more broadly people's reasonable expectations regarding privacy. Website or browser privacy settings, company advertising, statements, and other design elements have an influence on people's expectations.[216] Courts, however, will not go this far, and cases to date have focused mainly on violations of explicit promises in privacy policies or statutory requirements.

However, there is a basis in contract law to recognize thwarted expectations as a harm. When a party to a contract fails to perform a term in a contract, even if it is a matter of mere personal taste that lacks value, courts will still enforce the term. In construction contract cases, for example, the difference in the value of property with and without the plaintiff's preferences might be slight or nil. Instead of assessing damages based on the difference in actual value, courts assess damages for the "cost of completion" because the "fair market value of a home does not necessarily reflect the value to the homeowner."[217] As Judge Cardozo famously stated in *Jacob & Youngs, Inc. v. Kent,* in a construction contract, "[t]here is no general license to install whatever, in the builder's judgment, may be regarded as 'just as good.'"[218] These cases suggest that the failure to respect people's preferences is a cognizable harm even these preferences do not add any economic value. For many people, their privacy preferences are an important consideration about whether or not to use a particular service or product.

In contrast to contract law, the FTC readily enforces for violations of privacy policies. Under the FTC's enforcement of the prohibition on "deceptive" acts or practices under Section 5 of the FTC Act, the FTC has viewed broken promises in privacy notices to be sufficient for harm.[219] Deception need not just involve statements made in privacy notices, as the FTC has found other statements about privacy to be deceptive.[220] The very crux of deception as used in the context of broken promises is that the harm is in personal data being used in ways that differ from how companies informed people it would be used. One of us has

[214] Woodrow Hartzog, *Website Design as Contract,* 60 AM. U. L. REV. 1665 (2011).
[215] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1879 (2013).
[216] Woodrow Hartzog, *Website Design as Contract,* 60 AM. U. L. REV. 1665 (2011).
[217] Willie's Constr. Co. v. Baker, 596 N.E.2d 958 (Indiana Ct. of Appeals 1992); *see also* Lyon v. Belosky Construction, 247 A.D.2d 730 (N.Y. App. Div. 1998) (awarding "cost of performance" damages in part based on the observation that "the aesthetic appearance of the home, both inside and out, was of utmost importance to plaintiffs."); American Standard, Inc. v. Schectman, 80 A.D.2d 318 (N.Y. App. Div. 1981) (contractor's failure to complete work resulted in $3,000 diminution in value but $90,000 in damages was awarded).
[218] Jacob & Youngs, Inc. v. Kent, 230 N.Y. 239, 243 (1921).
[219] Daniel J. Solove & Woodrow Harzog, *The FTC and the New Common Law of Privacy,* 114 Colum. L. Rev. 583, 628-30 (2014).
[220] *Id.* at 630-33.

argued that the FTC could and should extend its jurisprudence further to pursue cases where people's expectations were thwarted even if no false statements are made.[221]

Critics claim that the FTC should curtail the extent to which it recognizes harm for thwarted expectations. James Cooper and Joshua Wright contend that the FTC has become undisciplined about how it recognizes privacy harms.[222] They argue that "unexpected data practices do not always equate to privacy harm."[223] They use an example of a smart oven app that records oven usage data, which is improperly shared with third parties. They argue that the FTC should not recognize harm in this case because the app's thwarting of privacy expectations "may be mediated through the market or the legal system."[224] They argue that "a focus on expectations, rather than harm, necessarily will be overly inclusive."[225]

The market, however, is not adequate to address the problems with the app. When people use an app that thwarts their privacy expectations, people's ability to assess the risks of using the app is impeded. The market cannot work fairly if people's expectations are completely wrong, if people lack knowledge of potential future uses of their personal data, and if people have no way to balance the benefits and risks of using products or services.

I. CONTROL HARMS

Many statutes provide certain rights or restrictions regarding the retention and use of personal data independently from what is promised in an organization's privacy policy. The harm for violations of these rights or restrictions is not thwarted expectations, as people might not have known about these statutes. Instead, the harm involves the loss of control over personal data.

Courts have been inconsistent in recognizing the loss of control as a harm. In *Braitberg v. Charter Communications*, for example, the Eighth Circuit denied standing to plaintiffs in a class action lawsuit against a cable company for failing to delete their personal data in violation of the Cable Communications Policy Act. The court concluded that the mere improper retention of data was not sufficient, by itself, to create a "material risk of harm."[226] In *Gubala v. Time Warner Cable, Inc.*, the court denied standing to a cable subscriber suing a cable company for improperly retaining personal data under the Cable Act because

[221] *Id.* at 667-69.
[222] James C. Cooper & Joshua D. Wright, *The Missing Role of Economics in FTC Privacy Policy*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 465, 479 (Jules Polonetsky, Evan Selinger, & Omer Tene, eds., 2017).
[223] *Id.* at 480.
[224] *Id.* at 480.
[225] *Id.* at 480.
[226] Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016).

there was no harm for merely holding data.[227] Similarly, in *Rivera v Google*, the court denied standing to plaintiffs who sued Google for storing their biometric data without their consent, a violation of the Illinois Biometric Information Privacy Act (BIPA). The court concluded that there was no harm because the data was not shared with anyone.[228] There are other courts that recognize the loss of control as a harm sufficient to justify standing.[229]

Losing control over our personal data constitutes an injury to our peace of mind and our ability to manage risk. In the clutches of organizations, personal data can be used for a wide array of purposes for an indefinite period of time. Privacy laws seek to regulate data flows to protect individuals from potential downstream uses. The practicalities of litigation, which are constrained by statutes of limitation, require an assessment of the situation before the end of the data life cycle.

Warren and Brandeis based their argument upon an English case from 1848 – *Prince Albert v. Strange*. This case involved a suit at equity to prevent William Strange from publishing a catalog describing etchings that the royal couple made about their family.[230] The court enjoined the publication of the catalog. Warren and Brandeis argued that the case involved the protection of "inviolate personality."[231] The case did not involve lurid images or embarrassing secrets (they were endearing hand drawn images of a mother with her child), and the couple had shared these personal etchings with loved ones.[232] Thus, the harm, as imagined by Warren and Brandeis, was the undermining of control over the extent to which personal information is circulated. This type of harm should be enough.

J. DATA QUALITY HARMS

Many privacy laws require that organizations adhere to the principle of "data quality" – keeping data accurate, complete, and up-to-date.[233] Courts are inconsistent in whether inaccuracies in data constitutes a cognizable harm.

In *Spokeo*, for example, the U.S. Supreme Court was skeptical about whether inaccurate data rose to the level of being cognizable. The plaintiff had

[227] Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2016).
[228] Rivera v Google, 366 F. Supp. 3d 998 (N.D. Ill. 2018).
[229] In contrast to *Grubala* and *Rivera*, the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corporation*, concluded that plaintiffs seeking relief under BIPA "need not allege some actual injury or adverse effect" to be considered aggrieved persons. *Rosenbach* diverges from *Grubala* and *Rivera* because it involves a holding that an actual injury is not required by the BIPA, and standing is not required in state court. Rosenbach v. Six Flags Entertainment Corporation et al., No. 123186, 2019 Ill. Lexis 7 (Ill. Jan. 25, 2019).
[230] Prince Albert v. Strange, (1849) 64 Eng. Rep. 293, 295 (Ch.).
[231] Warren and Brandeis, *supra* note X, at 205.
[232] See The Right to Privacy (2020).
[233] **CITES**

complained about errors in his consumer report that falsely stated that he was married and had professional degrees. The Court did not examine the specific errors that the plaintiff complained about. Instead, the Court spoke generally about errors: "An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[234] Unfortunately, the Court chose a rather poor example, as a lot can be inferred about a person based on their zip code. Numerous demographic generalizations can be made about many zip codes about race, religion, ethnicity, income, and more.

The Court remanded the case back to the Ninth Circuit to determine whether the errors in the plaintiff's records were sufficiently harmful. On remand, the Ninth Circuit held Robins had alleged a cognizable harm.[235] The court noted that accuracy and other components of data quality involved "interests protected by FCRA's procedural requirements are 'real,' rather than purely legal creations."[236] According to the court, "given the ubiquity and importance of consumer reports in modern life—in employment decisions, in loan applications, in home purchases, and much more—the real-world implications of material inaccuracies in those reports seem patent on their face."[237] Further, the court observed that "[c]ourts have long entertained causes of action to vindicate intangible harms caused by certain untruthful disclosures about individuals, and we respect Congress's judgment that a similar harm would result from inaccurate credit reporting."[238]

Finding specific economic harms for incorrect information in records can be challenging because errors or missions could lead to a variety of consequences at some point in the future, long beyond the statute of limitations for most causes of action. Suppose, for example, that a credit report erroneously states that a person went bankrupt. Whether the error causes any economic harm will depend upon how the report is used. A wise person would likely refrain from seeking a loan while the error remains in the report, as this could result in denial of the loan or a higher interest rate. For example, in *Sarver v. Experian*, the court held that the plaintiff failed to establish actual damages based on an inaccurate bankruptcy notation in his credit report before he tried to apply for credit from a third party. Afterwards, he could establish damages.[239] But to have courts recognize harm, should a person have to go through the charade of applying for a loan in order to generate proof of economic harm?

Inaccuracies create risk of future harm that are difficult to predict, but they are still harmful in the present day because they cause a loss of data hygiene.

[234] **CITE**
[235] Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017), cert. denied, 138 S. Ct. 931 (2018).
[236] *Id.*at 1114.
[237] *Id.*
[238] *Id.* at 1115.
[239] Sarver v. Experian, 390 F.3d 969 (7th Cir. 2004).

Imagine that someone that you invited into your house takes all your clothes out of the drawers and closets and throws them on the floor. The person removes all your books from the shelves and shoves them in a corner. The person tracks dirt all over your floors, though it does not permanently stain them. No structural damage is done to the house, but it is now a mess. You have been harmed even though the value of your home is not diminished. You have suffered a loss. You would likely find the mess and dirt in your home to be unpleasant. You might not invite guests over to your home until it is cleaned. The harm is not the diminishment in value of the house; it is interference with your enjoyment of your home as well as the time and expense to clean up the mess. When data is sullied with misleading or incorrect information, there is a similar mess – just one in digital space rather than in a physical place. And, unlike in real space, the contamination can be difficult to eradicate. It can be hard for individuals to find out about errors and when they do, third parties will ignore requests to correct them without the real risk of litigation costs.

K. INFORMED CHOICE HARMS

Courts are inconsistent about recognizing harm for failing to give individuals information to assist them in making informed choices about their personal data or exercise of privacy rights. In *Robertson v. Allied Solutions*, for example, the plaintiff Robertson applied for a job at Allied. Allied obtained a background check on Robertson. Although the FCRA requires that applicants be provided a copy of the report and information about their FCRA rights, Allied failed to provide either to Robertson. The Seventh Circuit held that she was harmed because she "was denied information that could have helped her craft a response to Allied's concerns."[240] Even if the information in the report is true, the court noted, a consumer might want to "bring additional facts to the employer's attention that put matters in a better light for the consumer.[241]

In *Long v. SEPTA*, an employer rejected applicants based on background checks that turned up information about convictions involving illegal drugs. Although FCRA requires that the applicants be provided a copy of their background check report and a written statement of their FCRA rights, SEPTA failed to provide these things.[242] The court concluded that the failure to provide a copy of the reports harmed plaintiffs by denying them the right to "see or respond" to them.[243] But regarding the failure to inform the applicants about their FCRA rights, the court concluded that they lacked standing because the plaintiffs knew their FCRA rights "to file this lawsuit within the prescribed limitations period, so they were not injured."[244]

[240] Robertson v. Allied Sols., LLC, 902 F.3d 690, 697 (7th Cir. 2018).
[241] Robertson v. Allied Sols., LLC, 902 F.3d 690, 696 (7th Cir. 2018).
[242] Long v. Southeastern Pa. Transp. Auth., 903 F.3d 312, 321 (3d Cir. 2018).
[243] *Id.* at 324.
[244] *Id.* at 325.

When individuals are not informed of their rights or not given important information, they are harmed because they lose their ability to assert their rights at the appropriate times, to respond effectively to issues involving their personal data, or to make meaningful decisions regarding the use of their data. Laws that mandate that people be informed of their rights are designed to empower individuals and arm them with appropriate knowledge. The holding in *Long* creates a closed circle where plaintiffs will never be able to enforce FCRA's rights disclosure requirement. If the plaintiffs do not know about their rights, then they likely will not know they can bring a lawsuit. If they bring a lawsuit, then courts will throw it out because they knew enough about their rights to sue. This closed circle all but forecloses enforcement of this provision.

In cases where people are not informed that their personal data was used to make a decision about them, they are harmed because informing them is to allow them to understand how their data affected a decision and to give them an opportunity to respond. This response might not be a direct refutation of the data. The response could take many forms, from providing additional data to explaining a situation to raising other unrelated considerations that might outweigh the negative impact of the data. Even if the response might fail to change minds, people should still have a chance to make their case. By way of analogy, denial of people's day in court is harmful even if they would likely have lost their case. The harm is in their losing their right to be heard.

L. VULNERABILITY HARMS

Courts are inconsistent in finding harm for failing to follow security safeguards that have not yet resulted in a data breach. For example, the FCRA mandates that no more than five digits from a credit card number can be printed on a receipt, but far more digits are printed on receipts in violation of the mandate. In cases where this provision is violated, some courts have held that there is an injury, and other courts have concluded that there is none.[245]

Consider these opposing findings. In *Muransky v. Godiva Chocolatier, Inc.*, the Eleventh Circuit held that printing more digits of a person's credit card on a receipt is an injury in fact because it is akin to a breach of confidentiality.[246] However, in *Bassett v. ABM Parking Services, Inc.*, the Ninth Circuit concluded that printing more credit card digits on a receipt was not a sufficient harm because Bassett did not allege that another copy of the receipt existed, that his receipt was lost or stolen, that he was the victim of identity theft, or even that another person apart from his lawyers viewed the receipt."[247]

---

[245] *Compare* Guarisma v. Microsoft Corp. with Bassett v. ABM Parking Servs., Inc., 883 F.3d 776 (9th Cir. 2018); Crupar-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76 (2d Cir. 2017); Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724 (7th Cir. 2016).

[246] Muransky v. Godiva Chocolatier, Inc., 922 F.3d 1175 (11th Cir. 2019).

[247] Bassett v. ABM Parking Servs., Inc., 883 F.3d 776, 783 (9th Cir. 2018).

At first blush, the *Basset* court notes a number of things that seemingly make the risk of future harm from the receipt low. But having the information on the receipt presents a risk if the receipt is lost or thrown away. The law's restriction of the digits on the receipt is not to shield the data from the customer who bought something and has the receipt. Instead, it is to enable everyone to be able to throw away receipts without having to worry about shredding them. This commitment promotes good security and alleviates the need for people to go to greater lengths to protect themselves.

In contrast to courts, the FTC has enforced against companies with inadequate security in the absence of a data breach. For example, in *In the Matter of Microsoft Corp.*, the FTC faulted Microsoft for failing to follow the promises it made about the security of a single login service.[248] In *In re Guess.com, Inc.*, the FTC enforced on a similar deception theory.[249] More recently, in *In the Matter of Zoom Video Communications, Inc.*, the FTC used an unfairness theory to fault Zoom for "limiting the intended benefit of a privacy and security safeguard provided by [the] Safari browser."[250] This created a "vulnerability" on users' computers, but the enforcement was not based on any malicious actors actually exploiting this vulnerability.

M. DISTURBANCE HARMS

Disturbance harms involve unwanted communications that disturb tranquility, interrupt activities, sap time, and otherwise serve as a nuisance. Many courts have held that unsolicited telephone calls and text messages in violation of the Telephone Consumer Protection Act (TCPA) constitute injuries in fact sufficient for standing. As one court explained, the harm can involve "wasting the consumer's time" and "interruption and distraction."[251] In *Van Patten v. Vertical Fitness Group,* for example, the Ninth Circuit noted that "[u]nsolicited telemarketing phone calls or text messages, by their nature, invade the privacy and disturb the solitude of their recipients."[252] Other TCPA cases are similar.[253] As the Fourth Circuit explained in *Krakauer v. Dish Network, LLC*,[254] the harm the TCPA addresses is receiving calls that people "previously took steps to avoid." Rejecting the notion that this harm was too intangible to be cognizable,

[248] In the Matter of Microsoft Corp., No. 012-3240 (Dec. 24, 2002).
[249] In re Guess Jeans, No. 022-3260 (July 30, 2003).
[250] In the Matter of Zoom Communications, Inc. (Nov. 19, 2020).
[251] LaVigne v. First Cmty. Bancshares, Inc., 215 F. Supp. 3d 1138, 1146 (D.N.M. 2016).
[252] Van Patten v. Vertical Fitness Grp., LLC., 847 F.3d 1037, 1043 (9th Cir. 2017) ("Unsolicited telemarketing phone calls or text messages, by their nature, invade the privacy and disturb the solitude of their recipients.").
[253] *See, e.g.*, Susinno v. Work Out World, Inc., 862 F.3d 346 (3d Cir. 2017) (holding that intangible injuries, such as nuisance and invasion of privacy, constituted the very harm that Congress sought to prevent in enacting the TCPA); Melito v. Experian Marketing Solutions, Inc., 923 F.3d 85, 88 (2d Cir. 2019) (holding that unsolicited text messages, like unwanted calls or faxes, constitutes the kind of nuisance and privacy harm that Congress identified when enacting the TCPA);
[254] Krakauer v. Dish Network, LLC, 925 F.3d 643 (4th Cir. 2019).

the court stated: "There is nothing ethereal or abstract about it."[255] Some courts, however, have rejected harm for certain types of communications under the TCPA, such as text messages. In *Salcedo v. Hanna*,[256] the Eleventh Circuit found that the receipt of a single text message does not constitute a concrete harm because a text message is different from a phone call or fax because a text message was nothing more than a momentary annoyance.[257] In contrast, in *Gadelhak v. AT&T Servs.*,[258] the Seventh Circuit concluded that unwanted text messages cause harm because the "undesired buzzing of a cell phone from a text message, like the unwanted ringing of a phone from a call, is an intrusion into peace and quiet in a realm that is private and personal, [which] is the very harm that Congress addressed [in TCPA]."[259]

Some courts have been skeptical of harm for the receipt of spam. In *Cherny v. Emigrant Bank*, the defendant bank improperly shared its customer email addresses with third parties, in violation of its privacy policy.[260] As a result, the plaintiff received spam. The plaintiff sued the bank based on breach of fiduciary duty and breach of contract. The court held that "[t]he receipt of spam by itself, however, does not constitute a sufficient injury entitling Cherny to compensable relief."[261]

N. AUTONOMY HARMS

Autonomy harms involve the restriction, coercion, or manipulation of people's choices. People are either directly denied free will to decide or are tricked into thinking that they are freely making choices when they are not. In the consumer privacy context, the most prevalent form of autonomy harm is "manipulation." Manipulation is a difficult harm to define, as there is a spectrum of ways to encourage people to think and act in certain ways, and some are deemed persuasion and others manipulation.

Ido Kilovaty contends that manipulation "impairs the ability of individuals to make independent and informed opinions and decisions. . . . It effectively deprives individuals of their agency by distorting and perverting the way in which individuals typically make decisions."[262] According Daniel Susser, Beate Roessler, and Helen Nissenbaum, manipulation "is a kind of influence--an attempt to change the way someone would behave absent the manipulator's interventions."[263] They distinguish manipulation from persuasion and coercion: "Persuading someone leaves the choice of the matter entirely up to them, while

[255] *Id.* at 653.
[256] 936 F.3d 1162 (11th Cir. 2019).
[257] *Id.* at 1167.
[258] 950 F.3d 458 (7th Cir. 2020)
[259] *Id.* n.1.
[260] Cherny v. Emigrant Bank, 604 F. Supp.2d 605 (S.D.N.Y. 2009).
[261] *Id.*
[262] Ido Kilovaty, *Legally Cognizable Manipulation*, 34 Berkeley Tech. L.J. 449, 469 (2019).
[263] Daniel Susser, Beate Roessler, and Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 Geo. L. Tech. Rev. 1 (2019).

coercing someone robs them of choice."[264] A coerced person understands that they are coerced where as a manipulated person might not realize that they are being turned into a puppet: "Coercion is blunt and forthright: one almost always knows one is being coerced. Manipulation is subtle and sneaky. Rather than simply depriving a person of options as the coercer does, the manipulator infiltrates their decision-making process, disposing it to the manipulator's ends, which may or may not match their own."[265] According to Cass Sunstein, manipulation involves "an effort to influence people's choices counts as manipulative to the extent that it does not sufficiently engage or appeal to their capacity for reflection and deliberation."[266]

In a survey of various definitions of manipulation, Shaun Spencer observes that they all share some common elements: "they all contain the notion of circumventing the subject's rational decision-making process" and most require intent to manipulate.[267] Drawing from these definitions, Spencer defines manipulation as "an intentional attempt to influence a subject's behavior by exploiting a bias or vulnerability."[268]

Ryan Calo contends that manipulation "creates subjective privacy harms insofar as the consumer has a vague sense that information is being collected and used to her disadvantage, but never truly knows how or when." Manipulation "also creates objective privacy harm when a firm uses personal information to extract as much rent as possible from the consumer."[269] According to Sunstein, the harm of manipulation "is that it can violate people's autonomy (by making them instruments of another's will) and offend their dignity (by failing to treat them with respect)."[270] Tal Zarsky contends that manipulation is harmful because "[m]anipulative practices impair the process of choosing, subjecting it to the preferences and influences of a third party, as opposed to those of the individuals themselves."[271]

Manipulation can affect not just individuals but also create societal harm, as people's decisions can affect not just themselves but society as well. The Cambridge Analytica incident involved the use of personal data on a mass scale to influence people's decisions in the 2016 U.S. presidential election and in the United Kingdom's vote for Brexit.[272]

The FTC has recognized that trade practices that prevent consumers from

---

[264] *Id.* at 15.
[265] *Id.* at 17.
[266] Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. Marketing Behavior 213, 218 (2015).
[267] Shaun Spencer, *The Problem of Online Manipulation*, 2020 U. Ill. L. Rev. 959, 989 (2020).
[268] *Id.* at 990.
[269] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995, 1029 (2014).
[270] Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. Marketing Behavior 213, **CITE** (2015).
[271] Tal Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES IN LAW 157, 174 (2019).
[272] **CITE**

"effectively making their own decisions" are ones that cause substantial injury. "Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[273]

When it comes to private litigation, manipulation has not been the subject of many privacy cases. As Cass Sunstein notes, "Because of the pervasiveness of manipulation, and because it often does little or no harm, the legal system usually does not attempt to prevent it."[274] Spencer is also skeptical about the law's ability to regulate manipulation because "it will be difficult, if not impossible, to establish that the allegedly manipulative stimulus caused the consumer harm."[275] People respond very differently to manipulation, and people might not even realize that they are being manipulated.

* * *

As we have pointed out above, the law is lacking in coherence and consistency regarding the recognition of cognizable privacy harms. Courts are often failing to recognize privacy harms and are thwarting the enforcement of privacy violations or leaving them unremedied. Our typology of privacy harms aims to help courts better understand why each type is harmful. We also have endeavored to show that there are concepts in other legal contexts that could be applied to recognize certain types of privacy harms.

III. THE CHALLENGES OF PRIVACY HARMS FOR THE COURTS

Although better recognizing privacy harms will improve the law's effectiveness at addressing privacy law violations, it is not enough. Privacy harms have a number of challenges that make litigating privacy cases difficult.

A. PRETEXTUAL HARMS

As a result of the current approach to harm, some courts locate harm in certain rather trivial costs or use of resources. Finding harm for these things is really a pretext for different types of harms that we have identified in Part II. Because courts require plaintiffs to allege tangible and concrete harms, complaints endeavor to lay out concrete harms that are not the heart of the matter at all. It is

[273] *Federal Trade Commission, Policy Statement on Unfairness* (1980), Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.
[274] Sunstein, *Manipulation, supra* note _, at X.
[275] Spencer, *Manipulation, supra* note __, at 997.

those harms that enable plaintiffs to get beyond motions to dismiss even though they are miniscule and do not capture why plaintiffs are suing.

One theory that has gained some traction is that plaintiffs suffered harm in losing device battery life and storage space based on broken promises.[276] In *In re iPhone Application Litigation*, plaintiffs alleged that Apple breached promises in its privacy policy to protect users' personal data because its operating system readily facilitated the non-consensual collection and use of their data by apps. The court found that plaintiffs had sufficiently alleged harm in claiming that the "unauthorized transmission of data from their iPhones taxed the phones' resources by draining the battery and using up storage space and bandwidth."[277]

In *Mey v. Got Warranty, Inc.*, the court held that unwanted calls to prepaid cell phones "cause direct, concrete, monetary injury by depleting limited minutes that the consumer has paid for" and also "deplete a cell phone's battery, and the cost of electricity to recharge he phone." The court noted that "[w]hile certainly small, the cost is real, and the cumulative effect could be consequential."[278] As another court noted, although the harm from "a single call or text (whether from depleted battery life, wasted time, or annoyance) would be de minimis," the Telephone Consumer Protection Act (TCPA) "is clear that a violation can occur from a single call."[279] As another court has noted: "Regardless of how small the harm is, it is actual and it is real."[280]

The actual harm to plaintiffs, however, is not lost storage space or slightly drained resources. These theories are invoked because they sound in a language that courts accept but not because they fit what plaintiffs suffered. The result is an odd sort of legal fiction, where the law redresses "harm" that is not the real interest interfered with as a means to redress a harm that really is.

The law fails to focus on what matters most, which is whether certain practices cause significant problems. Lucky plaintiffs can conjure up some sort of minor tangible impact. But plaintiffs who can point to a severe problem that does not involve a negligible tangible impact are out of luck. The law perversely redresses trivial things rather while ignoring major problems.

B. AGGREGATION OF SMALL HARMS

A major complicating dimension of many privacy harms is that they are small but numerous. When these harms happen to an individual repeatedly by different actors, they become significantly more harmful. For example, receiving an

[276] Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012); Anderson v. Hannaford Bros., 659 F.3d 151 (1st Cir. 2011).
[277] In re IPhone Application Litig., 844 F.Supp.2d 1040 (E.D. Cal. 2012).
[278] Mey v. Got Warranty, Inc., 193 F. Supp. 3d 641, 644-45 (N.D. W. Va. 2016); *see also* Martinez v. TD Bank USA, N.A., 225 F. Supp. 3d 261, 270 (D.N.J. 2016).
[279] Etzel v. Hooters of Am., LLC, 223 F. Supp. 3d 1306, 1312 (N.D. Ga. 2016).
[280] LaVigne v. First Cmty. Bancshares, Inc., 215 F. Supp. 3d 1138, 1146 (D.N.M. 2016).

unwanted email is a minor inconvenience. Receiving hundreds of unwanted emails becomes a major imposition and distraction.

Another aspect of this difficulty is that sometimes an organization will cause a very small amount of harm but on a very large scale – to millions or even billions of people. From the standpoint of each individual, the harm is minor, but from the standpoint of society, where the harm to everyone is aggregated, the total amount of harm is quite substantial.

Privacy harms often involve the aggregation of many small harms to each individual, which is compounded by the aggregation of all these harms to many individuals. The result makes privacy violations large-scale problems that cause a significant societal impact, but that do not fit readily into the traditional way the law looks at harm.

FTC enforcement has successfully addressed the problem. In its policy statement about unfairness injury, the FTC has noted: "An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[281]

However, when it comes to private litigation, for each individual, bringing a lawsuit for a small harm is not be worth the time or resources. Class actions are the predominant way to address this problem. Class actions allow for many people to aggregate their small harms into a single lawsuit that is large enough to justify the costs of litigating it.

Class actions, however, are an imperfect vehicle to address privacy problems. Cases often quickly settle because the cost of litigating them is high. The lawyers often earn significant sums, maximizing their own financial interests.[282] Many class actions become the equivalent to a shake down, with companies paying the lawyers to go away.

If class actions do not settle, there is another problem. Companies have data on millions or billions of people, and even small damages can add up to enormous sums that can put companies out of business. These sums can become disproportionate to what the company did wrong. Judges are reluctant to recognize harm because it might mean bankrupting a company just to give each person a very tiny amount of compensation.

---

[281] *Federal Trade Commission, Policy Statement on Unfairness* (1980), Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984) at n.12, http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[282] Eric Goldman, *The Irony of Class Action Privacy Litigation*, 10 J. Telecomm. & High Tech. L. 309, 314 (2012).

C. UNKNOWABLE AND FUTURE HARMS

In many cases, the harm is not fully knowable. For data breach harms, a major complication is that plaintiffs have not yet suffered from identity theft or fraud. Plaintiffs argue that they suffer harm in the form of a future risk of injury. Courts are wildly inconsistent in recognizing future risk of injury as a cognizable harm.[283]

Privacy harms often not only involve a future risk of injury, but they are compounded by an additional dimension of complexity: the range of possible future injuries is much more varied and could be anything in the typology of privacy harms that we have set forth above. To fully understand the implications of the collection, use, or disclosure of personal data, one must know about the future uses to which the data will be put. For example, if Company A improperly discloses personal data to Company B, the harm will depend upon what Company B does with the data. Company B might not immediately use the data in a harmful way and might not do so until after the statute of limitations. Company B might never use the data in a harmful way.

Privacy harms are highly contextual, with the harm depending upon how the data is used, what data is involved, and also how the data might be combined with other data. Sharing an innocuous piece of data with another company might provide a key link to other data or allow for certain inferences to be made.

Because of these difficulties, many privacy statutes use statutory damages. It is far easier to enforce laws with statutory damages than to try to figure out the harm which may involve future uses that may or may not occur. Through standing doctrine and cases like *Spokeo,* however, courts are undermining statutory damages provisions by forcing tired old judicial concepts of harm into the enforcement of these statutes. For cases not involving statutes with statutory damages, harm can become quite a speculative matter if there is uncertainty in two dimensions – the possibility of harm and the nature of harm.

D. INDIVIDUAL VS. SOCIETAL HARMS

Privacy harms often involve injury not just to individuals but to society. As a number of scholars have argued, privacy is "constitutive" of society.[284] As Joel Reidenberg contends, [s]ociety as a whole has an important stake in the contours of the protection of personal information."[285] Robert Post argues that the privacy torts promote "rules of civility that in some significant measure constitute both

[283] Solove and Citron, *Risk and Anxiety, supra* note _, at X.
[284] *See, e.g.,* PRISCILLA M. REGAN, LEGISLATING PRIVACY (1995) (arguing that privacy should be understood in terms of its social benefits); Spiros Simitis, *Reviewing Privacy in an Information Society,* 135 U. Pa. L. Rev. 707, 709 (1987) ("[P]rivacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone.").
[285] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies,* 54 Hastings L.J. 877, 882-83 (2003).

individuals and community."[286] According to Julie Cohen, privacy protects individual autonomy and creativity that are essential for society to develop a rich culture.[287] Paul Schwartz contends that privacy is essential to democracy and freedom.[288]

These considerations are often omitted from the law's evaluation of harm because they do not fit the individualistic focus that courts have for cognizable harm. Although certain lawsuits seek mainly to vindicate individual interests, many group lawsuits (such as class actions) also seek to protect broader societal interests. Courts, however, often still fail to consider the societal impact of privacy harms even in these cases.

IV. REALIGNING PRIVACY ENFORCEMENT AND REMEDIES

With the law's relentless focus on privacy harms in so many contexts that result in the dismissal of suits, it is easy to overlook the broader challenges afoot. Privacy harms are just a piece of a larger pie involving the enforcement of privacy law. In addition to the question of what should constitute cognizable privacy harm, we should also ask whether privacy harm should even be required in particular circumstances. In many cases, harm is irrelevant to the purposes of the litigation. To determine when privacy harm is an issue that should even be part of a case, we must answer a broader overarching question: *When and how should privacy law be enforced?*

Many of the law's difficulties with handling privacy cases are due to misalignments between enforcement goals and remedies. Configuring the proper alignment will make the law more coherent and effective.

Privacy law enforcement has three predominant goals:

(1) Compensation – compensating people who have been harmed
(2) Deterrence – preventing future violations of the law
(3) Equity – making things right by means other than compensation

Problems emerge when a remedy is misaligned with an enforcement goal. For example, monetary damages are a proper remedy when compensation is the goal. They are not a well-tailored remedy when deterrence or equity is the goal. The law becomes messy and riddled with problems when it tries to use the same remedy to address different goals. It is understandable why the law tries to do

[286] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Calif. L. Rev. 957, 959 (1989).
[287] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1428 (2000).
[288] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L Rev. 1609, 1613 (1999)

this: sometimes multiple enforcement goals exist in the same case. But trying to use a remedy well-suited for one goal but ill-suited for another is a recipe for failure.

An analogy can deepen our understanding of the point. A wrench is a great tool for unscrewing a nut. One could also try to use a wrench to hammer in a nail, but a wrench is a poor tool to use, as it might cause damage. The nail requires a hammer for its installation. The law is akin to a bad repairperson; it is constantly trying to use the wrong tools to achieve enforcement goals. Just because in a given situation there is a nut to unscrew and a nail to be hammered does not mean that only a wrench or a hammer should be used. *Both* tools should be used.

This point might seem obvious, but the law almost entirely misses it. Modern tort law is premised on the notion that lawsuits to compensate people with damages can also double as a means to achieve deterrence. Of course, it is certainly true that compensatory damages can further the goal of deterrence, but this is akin to the use of the wrench to hammer in the nail – the wrench can be used, but it is the wrong tool, and it will not work optimally. In privacy cases, because of the challenging nature of privacy harms, the misfit in tools is exacerbated.

A. THE GOALS OF ENFORCEMENT

Understanding the goals of enforcement is essential to making progress toward the effective enforcement of privacy law. Compensation involves awarding a plaintiff with monetary damages to provide redress for harm wrongfully caused. The typical tort rule accords with this rationale by awarding damages equal to a victim's loss.[289] Corrective justice theory embraces an Artistotelian concept of justice that requires injurers to make victims whole.[290] The goal is to hold actors responsible for losses that they wrongfully caused.[291]

Deterrence involves imposing a penalty that deters future wrongdoing. Specific deterrence involves deterring wrongdoing by the particular wrongdoer against whom enforcement is sought. General deterrence involves deterring wrongdoing by other actors. The penalty imposed on a particular wrongdoer will serve as a lesson to teach others to avoid wrongdoing. Many organizations will only take laws seriously when there are likely and painful consequences for failing to comply.

Equity involves righting wrongs in situations where compensation is not an adequate way of addressing them. Equitable remedies aim to restore things to their original state before the wrongdoing or to help fix situations where

[289] Id.

[290] JULES COLEMAN, RISKS AND WRONGS 320 (1992); ERNEST J. WEINRIB, THE IDEA OF PRIVATE LAW 56-57 (1995).

[291] JULES COLEMAN, THE PRACTICE OF PRINCIPLE 15, 36 (2001).

damages will not. The law has a number of equitable remedies, such as injunctions and specific performance.

B. ALIGNING REMEDIES WITH GOALS

1. The Problem of Misalignment

The law suffers when it fails to align appropriate remedies with enforcement goals. When compensation is the enforcement goal, compensatory damages are the appropriate remedy, and these damages are based on harm. When deterrence is the enforcement goal, private rights of action enable "private attorneys general" to enforce a law. Compensatory damages are a misfit in many cases unless there is harm. The remedy should be an amount that provides optimal general and specific deterrence. When equity is the enforcement goal, appropriate equitable remedies should be used. Harm should not be required. The main issue should be whether there is a problem that can be fixed or ameliorated with legal intervention.

Tort law attempts to achieve both the goal of compensation and deterrence simultaneously. This attempt to do both might seem efficient, but the goals are quite different. For example, when lawsuits are tied to compensatory damages, the existence of liability insurance can complicate the goal of deterrence. When the magnitude of the defendant's insurance premiums does not track the magnitude of the defendant's liabilities, the threat of liability may fall short of promoting optimal deterrence because the defendant can externalize the risk of liability through the purchase of insurance.[292]

On the flip side, liability for compensatory damages can be far greater than is optimal for deterrence. Compensation even for very small harms can become outsized if multiplied by millions of people. Deterrence is the more meaningful goal, and compensation in these instances might be counterproductive. For example, providing a few cents to a billion individuals might do little for their social welfare, but could put companies out of business. It might result in over-deterrence, leading companies to abandon socially beneficial personal data practices.

In many instances, private litigation is used primarily as a vehicle to achieve deterrence. Legislatures often include a private right of action in statutes so that plaintiffs acting as "private attorneys general" will help enforce the law. The goal is to increase enforcement to deter violations. The use of the private right of action for compensation is a secondary goal or a goal in only a small number of cases. As the Illinois Supreme Court noted in *Rosenbach v. Six Flags*

---

[292] KENNETH S. ABRAHAM, DISTRIBUTING RISK: INSURANCE, LEGAL THEORY, AND PUBLIC POLICY 64-83 (1986); Kenneth S. Abraham & Lance Liebman, *Private Insurance, Social Insurance, and Tort Reform: Toward a New Vision of Compensation for Illness and Injury*, 93 Colum. L. Rev. 75, 86 (1993).

Entertainment Corporation regarding the Illinois Biometric Information Privacy Act (BIPA), harm is not a requirement of the statute, and the legislature included the private right of action not just to compensate plaintiffs but because it "is as integral to implementation of the legislature's objectives" to deter BIPA violations.[293]

Sone courts, however, miss the point about private attorneys general. For example, in *Stoops v. Wells Fargo,* plaintiff Melody Stoops bought 35 cell phones to try to ensnare companies that made telemarketing calls in violation of the TCPA. The TCPA provides penalties of $500 for each violation with penalties trebled for willful or knowing violations.[294] The court dismissed her case for lack of harm: "Plaintiff's privacy interests were not violated when she received calls from Defendant. . . Because Plaintiff has admitted that her only purpose in using her cell phones is to file TCPA lawsuits, the calls are not 'a nuisance and an invasion of privacy.'"[295] According to the court, "Plaintiff has not suffered an injury-in-fact because her privacy and economic interests were not violated when she received calls from Defendant." The court reasoned that "it cannot reasonably be assumed that Congress intended to permit the suit" and that "it is unfathomable that Congress considered a consumer who files TCPA actions as a business when it enacted the TCPA."[296]

Stoops may have been opportunistic, but her motives does not negate the harm inflicted upon her. Trying to catch a wrongdoer does not mean that one is unharmed by the wrongdoer's actions in the process. Ultimately, however, harm should not be relevant to the *Stoops* case. Congress wrote the private right of action under the TCPA without a requirement of harm. Deterrence is the goal, not compensation. The fact that lawyers and plaintiffs benefit financially from enforcing privacy laws is a necessary side effect of private rights of action. Litigation must be sufficiently remunerative to incentivize private enforcement.

Contrary to the court's view of Stoops, she was engaging in desirable enforcement of the TCPA, catching violators when enforcement agencies were not. The main benefit of a private right of action in a law is to encourage private enforcement of that law. Because government agencies often lack the resources to enforce a law rigorously and consistently enough.

2. An Approach for Realignment

In privacy cases, how should the law better align the goals of enforcement with remedies? When should harm be required? We contend that harm should be an

[293] Rosenbach v. Six Flags Entertainment Corporation et al., No. 123186, 2019 Ill. Lexis 7 (Ill. Jan. 25, 2019).
[294] 47 U.S.C. §227(c)(5).
[295] Stoops v. Wells Fargo, 197 F.Supp.3d 782 (W.D. Pa., June 24, 2016).
[296] *Id.* (citations and internal quotations omitted).

issue only in cases where the enforcement goal is compensation. In many instances of privacy litigation, the enforcement goals involve deterrence and equity, not compensation. For these cases, harm is irrelevant. The amount of damages in such cases should be tailored to the enforcement goal. When the goal is deterrence, attempting to conjure up some amount of compensation (often based on pretext) will not be optimal for achieving this goal. The issue of harm just gets in the way and muddies the waters when the essential issue is clear: *What amount of damages would be optimal for deterrence?* For cases where equity is the goal, non-monetary remedies should be imposed. Redressing harm can certainly be one of the aims of equity, but goals of equity extend far beyond traditional conceptions of harm. Equity is a way to right wrongs, not just remedy harms.

More specifically, we propose the following approach: First, courts should require harm in tort actions brought to secure compensation. Establishing harm should be restricted only to the ability to obtain compensatory damages. Other relief, such as equitable relief, should not turn on harm.

Second, for contract cases, courts should enforce the contract. Courts should use remedies, such as specific enforcement, restitution, or recission. Attorneys fees and some modest damages should be paid to compensate for the time and hassle of having to litigate to make the defendant adhere to the contract.

Third, courts should not inject harm into cases involving statutes with private rights of action. Modern standing doctrine has strayed too far from the Constitutional requirement of "cases" or "controversies" to shut the doors to the courts to many cases that should be heard. Standing has become a conceptual mess, with courts spending too much time questioning harm and losing sight of the important issues.

Standing doctrine is a significant impediment to the coherent operation of privacy laws. Standing forces harm into cases where it should not be. *Spokeo* is part of a lineage of Supreme Court cases that shifted to a harms-based approach as a mechanism to shut off courts as a means for achieving social justice. According to Cass Sunstein, modern standing doctrine is an attack on the enforceability of much modern regulation: "[T]he very notion of 'injury in fact' is not merely a misinterpretation of the Administrative Procedure Act and Article III but also a large-scale conceptual mistake."[297] Sunstein argues that the injury-in-fact requirement "injects common law conceptions of harm into the Constitution."[298] It purports to be a "purely factual inquiry" but is "inevitably a product of courts' value-laden judgments."[299]

[297] Cass R. Sunstein, What's Standing After Lujan? Of Citizen Suits, "Injuries," and Article III, 91 Mich. L. Rev. 163, 167 (1992).
[298] *Id.* at 167.
[299] *Id.* at 167.

Likewise, Felix Wu argues that "standing law seems to be serving no purpose other than to constitutionalize a deregulatory agenda."[300] "Until recently," Wu observes, "tangibility and other questions about the quality of the harm suffered by the plaintiff simply were not part of the Supreme Court's standing analysis. Lower courts nevertheless incorporated such considerations into their analyses of standing in privacy cases. The Supreme Court has now done the same, thus shifting the law on standing, while professing that nothing has changed."[301] As Rachel Bayefsky notes, before the shift in standing doctrine, instead of requiring harm, courts required merely a "legal right" to bring a lawsuit based on property, contract, tort, or statute.[302]

Spokeo's invitation to courts to look to historically recognized harms in the common law further ossifies the common law's protection of privacy beyond the ossification caused by Prosser.[303] Warren and Brandeis aimed to generate new causes of action to rise to the problems; ossification contravenes the very spirt of their article. For Warren and Brandeis, the common law looks not just backwards but forwards as well. The common law is progressive, not regressive.

The requirement of harm in standing that overrides private rights of action in laws invites judicial overreaching. Courts should approach statutory private rights of action with more humility. Legislatures do not provide private rights of action loosely. Private rights of action are one of the most contested elements of laws, and when legislatures deem that violations of a law require the recognition of private rights of action, judges ought to show more respect for the legislature's determination.

Nullifying this enforcement component of the law can thwart the way the law is supposed to work. When Congress passes statutes, it will sometimes preempt state laws on the same issue, so plaintiffs might be barred from suing in state court for state law violations. Preemption is a kind of bargain, where plaintiffs might lose out on pursuing actions in state court but will be allowed instead to pursue actions in federal court based on the federal statute. This is how FCRA works, as it preempts certain state laws and directs plaintiffs to sue under its provisions.[304] By requiring harm, courts pull the rug out from that bargain, leaving plaintiffs with nowhere to pursue their cases.

Congress weighs various enforcement mechanisms from agency enforcement to state attorney general enforcement to private rights of action. Many statutes have a mix of different types of enforcement, presumably because it is Congress's

---

[300] Felix T. Wu, *How Privacy Distorted Standing Law*, 66 De Paul L. Rev. 439, 440 (2017).
[301] Felix T. Wu, *How Privacy Distorted Standing Law*, 66 De Paul L. Rev. 439, 439-40 (2017).
[302] Rachel Bayefsky, Constitutional Injury and Tangibility, 59 Wm. & Mary L. Rev. 2285, 2295 (2018).
[303] Matthew S. DeLucala, Note, The Hunt for Privacy Harms After *Spokeo*, 86 Fordham L. Rev. 2439, 2463-68 (2018).
[304] FCRA, 15 U.S.C. §1681h (permitting state tort actions only when defendants act with "malice or willful intent to injure plaintiff").

judgment about the efficacy of a particular enforcement mix. When courts nullify a component of Congress's enforcement mix, this can throw off the statutory recipe in ways that Congress did not anticipate.

Focusing on individual harm for these latter types of lawsuits is missing the point and actual purpose of the lawsuit. Many class action lawsuits would not be worth the significant costs if their sole benefit were to compensate individuals for any harm. For many class action lawsuits, the amount of compensation individuals receive is trivial. If this were the main benefit of these lawsuits, then we ought to reconsider whether they are worth the costs. The real value of many class action lawsuits is in holding defendants accountable for their wrongdoing when the harm is of a nature that is small and dispersed.

The law must break away from the rigid formalistic approach that anytime there is even a very small harm, it warrants compensatory damages. The law should also eschew its rigidity in dismissing cases when there is no cognizable harm. The rigidity makes litigation fit quite poorly with enforcement goals.

In class action cases where there may be only a small harm to individuals, courts should be able to fashion a remedy without resorting to compensatory damages. Compensatory damages for large classes could end up adding to an excessive sum beyond that necessary to achieve the optimal deterrence. A miniscule amount of damages for each class member will not address the goal of compensation in a meaningful way. In such a situation, the enforcement goal is the meaningful one, and this goal should be the driver of the appropriate remedy.

In other cases, the amount of compensatory damages might be too low for optimal enforcement. If the compensation to the class is minimal, then compensatory damages are not a meaningful remedy, and courts should be able to fashion a more appropriate remedy with punitive damages or equitable relief.

To avoid unnecessary class action lawsuits, in statutory cases where only deterrence is a goal, and compensation is not involved, courts might be given the option of evaluating the extent to which the statute has already been enforced. If a regulatory agency has already enforced a law effectively for the violation, then the statute might have a requirement for establishing harm, as the only goal of a lawsuit under these circumstances would be compensation. Legislatures could write laws to permit courts to dismiss lawsuits in situations where regulatory enforcement has been sufficient for deterrence and other enforcement goals are not present.

V. CONCLUSION

A well-calibrated legal response to privacy cases would permit socially beneficial personal data practices while requiring robust protections for the handling of personal data. Its primary focus should be on the deterrence of violations with the goal of encouraging widespread compliance. Compensation is important for individuals who have suffered significant harm.

Legal intervention should be designed to ensure that socially beneficial information practices continue. Our economy depends upon the collection and sharing of personal data. At the same time, personal data practices are inherently risky. Privacy law aims to ensure that personal data is used properly, that individuals have the ability to make decisions about their personal data, that there are meaningful guardrails and boundaries about how data is collected, used, or disclosed.

But struggles with recognizing cognizable privacy harms have impeded the law's effectiveness. Crabbed conceptions of harm have led courts to dismiss cases that are a key lynchpin for privacy law enforcement.

The common law as well as litigation of private rights of action have much to contribute to the development of privacy regulation. The common law remains underdeveloped. There are many helpful concepts in the common law that can advance privacy protection in a useful way. Although currently, the common law privacy has failed to develop adequate protections of privacy in the digital age, the common law could certainly do so in the future. The common law has doctrines, concepts, and remedies that could be very effective tools for privacy law.

Private litigation can play a major role in effective privacy law enforcement, and there are foundations in the law for it to develop in productive ways. For example, one of us has contended that strict liability has been underutilized in privacy cases.[305] Strict liability obviates proving fault, and the vast repositories of personal data that are being maintained about people can be analogized to the ultrahazardous activities of the Industrial Age. Lauren Scholz argues that restitution is a viable remedy for many privacy violations.[306] Restitution involves returning back benefits that unjustly enriched a defendant. Scholz also recommends that "[g]iven the cramped nature of the privacy torts, a better avenue for tort law for data trafficking lies in torts related to wrongful business practices. This family of torts has the aim of promoting basic fair play in commerce."[307] Scholars have recommended developing the protections of fiduciary relationships to apply to companies that process personal data,

[305] Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age. 80 S. Cal. L. Rev. 241 (2007).
[306] Lauren Henry Scholz, *Privacy Remedies,* 94 Ind. L.J. 653 (2019)
[307] *Id.* at 668.

including one of the authors of this article.[308] Moreover, various federal statutes lacking a private right of action can still serve as the basis for the standard of care in common law tort actions, such as UDAP laws, negligence, breach of confidentiality, and others.[309]

The requirement of harm has been a significant impediment to the law's development. The rigid clinging to an approach where enforcement goals and remedies are misaligned results in cases that lead to poor outcomes. With the proper alignment, a broader recognition of privacy harms, a better understanding of privacy problems, and a more flexible approach, the law can more effectively protect privacy in ways that are fair to all stakeholders.

[308] SOLOVE, THE DIGITAL PERSON, *supra; Solove & Richards, Privacy's Other Path* ***CITE****; Balkin, Information Fiduciaries, supra;* Lauren Henry Scholz, *Fiduciary Boilerplate*, __ J. Corp. L. __ (June 5, 2020), available at https://ssrn.com/abstract=3620164.

[309] *See infra* at text accompanying notes __.