Risk and Anxiety: A Theory of Data-Breach Harms

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

In lawsuits about data breaches, the issue of harm has confounded courts. Harm is central to whether plaintiffs have standing to sue in federal court and whether their legal claims are viable. Plaintiffs have argued that data breaches create a risk of future injury, such as identity theft, fraud, or damaged reputations, and that breaches cause them to experience anxiety about this risk. Courts have been reaching wildly inconsistent conclusions on the issue of harm, with most courts dismissing data-breach lawsuits for failure to allege harm. A sound and principled approach to harm has yet to emerge.

In the past five years, the U.S. Supreme Court has contributed to the confusion. In 2013, the Court, in Clapper v. Amnesty International, *concluded that fear and anxiety about surveillance—and the cost of taking measures to protect against it—were too speculative to satisfy the "injury in fact" requirement to warrant standing. This past term, the U.S. Supreme Court stated in* Spokeo v. Robins *that "intangible" injury, including the "risk" of injury, could be sufficient to establish harm. When does an increased risk of future injury and anxiety constitute harm? The answer remains unclear. Little progress has been made to harmonize this troubled body of law, and there is no coherent theory or approach.*

In this Article, we examine why courts have struggled to conceptualize harms caused by data breaches. The difficulty largely stems from the fact that data-breach harms are intangible, risk-oriented, and diffuse. Harms with these characteristics need not confound courts; the judicial system has been recognizing intangible, risk-oriented, and diffuse injuries in other areas of law. We argue that courts are far too dismissive of certain forms of data-breach harm and can and should find cognizable harms. We demonstrate how courts can

---

* John Marshall Harlan Research Professor of Law, George Washington University Law School. We are grateful to Ryan Calo for thoughtfully responding to our work and to *Texas Law Review* for inviting the conversation. Thanks to Catharine Sharkey, Deven Desai, Will DeVries, Susan Freiwald, Woodrow Hartzog, Chris Hoofnagle, Margot Kaminski, Gregory Keating, Orin Kerr, William McGeveran, Joel Reidenberg, Felix Wu, and the participants at the Privacy Law Scholars Conference for helpful comments. We would like to thank Kristen Bertch, Ariel Glickman, Cassie Meijas, Susan McCarty, and Austin Mooney for their research assistance. We are grateful to the editors of the Texas Law Review for their superb assistance.

** Morton & Sophia Macht Professor of Law, University of Maryland Francis King Carey School of Law; Affiliate Fellow, Yale Information Society Project; Affiliate Scholar, Stanford Center on Internet & Society.

assess risk and anxiety in a concrete and coherent way, drawing upon existing legal precedent.

Introduction

Suppose that Company X fails to adequately secure its clients' personal data. Imagine the company knows that hackers previously accessed its system yet does nothing about it. This time, hackers have little difficulty accessing the company's computer network to steal sensitive personal data about thousands of individuals. In the hackers' hands are now the keys to those individuals' credit and bank accounts: Social Security numbers, birth

dates, and financial information. The company's clients bring suit, seeking compensation for their increased risk of identity theft, the money they spent monitoring credit activity, and the ensuing emotional distress.

The defining issue in this lawsuit will be harm. If plaintiffs bring suit in federal court, they will have to demonstrate that they suffered harm sufficient to establish Article III standing.[1] Beyond the hurdle of standing, plaintiffs will have to establish harm to recover under tort, contract, or other claims in both federal and state courts.

In the past two decades, plaintiffs in hundreds of cases have sought redress for data breaches caused by inadequate data security.[2] In most instances, there is evidence that the defendants failed to use reasonable care in securing plaintiffs' data. The majority of the cases, however, have not turned on whether the defendants were at fault. Instead, the cases have been bogged down with the issue of harm. No matter how derelict defendants might be with regard to security, no matter how much warning defendants have about prior hacks and breaches, if plaintiffs cannot show harm, they cannot succeed in their lawsuits.

The concept of harm stemming from a data breach has confounded the lower courts. There has been no consistent or coherent judicial approach to data-breach harms. More often than not, a plaintiff's increased risk of financial injury and anxiety is deemed insufficient to warrant recognition of harm,[3] even though the law has evolved in other areas to redress such injuries.

---

1. Gladstone Realtors v. Village of Bellwood, 441 U.S. 91, 99 (1979). The issue of standing also comes up in state courts adjudicating data-breach claims. *See, e.g.*, Maglio v. Advocate Health & Hosps. Corp., 40 N.E.3d 746, 753–55 (Ill. App. Ct. 2015) (explaining that federal standing principles are similar to those in Illinois and in turn dismissing data-breach claims under Illinois law because the risk of identity theft and emotional distress did not amount to injury in fact sufficient to support standing).

2. *See* Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 93 (2014) (noting the 231 federal data-breach lawsuits from 2000–2011).

3. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40, 43 (3d Cir. 2011) (finding that increased risk of identity theft is too speculative a harm in a case involving the theft of personal data); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 849–50, 854–55 (S.D. Tex. 2015) (same); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015) (same); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25, 28 (D.D.C. 2014) (same); Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 470–71 (D.N.J. 2013) (same). *But see* Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388 (6th Cir. 2016) (recognizing that increased risk of identity theft and reasonably incurred mitigation costs to avoid future harm were sufficient for standing because hackers allegedly had stolen plaintiffs' information and the defendant offered free credit monitoring services to help consumers mitigate danger); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967, 969 (7th Cir. 2016) (concluding that there was a substantial risk of harm and mitigation costs to suffice as injury for standing); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (stating that increasing the future risk of harm can be sufficient for injury in fact); *In re* Home Depot Customer Data Sec. Breach Litig., No. 1:14-md-2583-TWT, 2016 WL 2897520, at *1, *3 (N.D. Ga. May 17, 2016) (finding harm to the plaintiffs (financial institutions) to warrant standing in a case concerning hackers' breach of Home Depot's databases because the plaintiffs incurred costs to avoid future harm including costs to cancel and reissue cards, costs to investigate fraudulent

The courts' refusal to recognize data-breach harms is, in no small part, due to confusion created by the Supreme Court decision in *Clapper v. Amnesty International USA*.[4] In *Clapper*, attorneys, journalists, and human-rights activists challenged the constitutionality of a provision of the Foreign Intelligence Surveillance Act (FISA), which expanded the government's authority to conduct surveillance over suspected terrorists.[5] Because the plaintiffs' work involved communicating with foreign individuals who might be deemed suspicious by the government, the plaintiffs believed that their communications would be monitored.[6] They spent significant money and time protecting the confidentiality of these communications, such as traveling abroad to speak with clients rather than talking to them on the phone.[7]

As the Court in *Clapper* explained, standing requires plaintiffs to have suffered an "injury in fact"—injury that is concrete, particularized, and actual or imminent (as opposed to hypothetically possible).[8] The Court acknowledged that the plaintiffs' theory of harm might be correct, but found that there was no proof that surveillance had, in fact, happened or was about to occur (or even that there was a substantial risk of its occurring in the future).[9] The proof sought by the Court was absent because, according to the government, the surveillance program had to be kept secret.[10] Thus, because the plaintiffs had no definitive way to find out about the surveillance until Edward Snowden forced the government's hand months later, the harm was merely conjectural.[11] The Court held that the plaintiffs lacked standing to sue because they could not show that the actual injury of government surveillance was underway or "certainly impending."[12] The plaintiffs' case was remanded

charges, costs for customer fraud monitoring, and costs due to lost interest and fees due to reduced card usage).

4. 568 U.S. 398 (2013).

5. *Id.* at 401, 427.

6. *Id.* at 401.

7. *Id.* at 406–07. For a thoughtful analysis of *Clapper*, see Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935, 1963 (2013) (criticizing the Supreme Court's decision in *Clapper* and arguing for the adoption of principles to guide the future development of surveillance law in order to balance the costs and benefits of government surveillance).

8. *Clapper*, 568 U.S. at 409.

9. *Id.* at 421–22.

10. Brief for Petitioner at 35, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (No. 11-1025); *see Clapper*, 568 U.S. at 412 & n.4 (insisting the burden to plead specific facts remained on plaintiffs despite the secrecy of those facts).

11. *See id.* at 412 ("Moreover, because § 1881a at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear, respondents' allegations are necessarily conjectural.").

12. *Id.* at 422.

because the plaintiffs could only speculate about whether their communications were under surveillance.[13]

Although the *Clapper* Court focused on the fact that the plaintiffs could not show that government surveillance was imminent or certainly impending, it stated in a footnote that "[i]n some instances," a "substantial risk that the harm will occur" would be sufficient to confer standing upon a plaintiff.[14] The Court failed to elaborate more on this point.

In decision after decision, courts have relied on *Clapper* to dismiss data-breach cases. For example, in *Reilly v. Ceridian Corp.*,[15] the case upon which the opening hypothetical is based, the Third Circuit held that the plaintiffs did not suffer harm because their "conjectures" about being victimized by identity theft or fraud had not yet "come true."[16] Plaintiffs' concerns about increased risk of identity theft and their outlay of money to protect against such theft were based "on entirely speculative, future actions of an unknown third-party."[17] Because thieves had not yet misused the plaintiffs' data, there was no "actual" harm to warrant standing or redress.[18] The court summarily rejected the plaintiffs' emotional distress claims for lack of standing.[19]

Much like *Reilly*, the majority of courts have ruled that injuries from data breaches are too speculative and hypothetical, too reliant on subjective fears and anxieties, and not concrete or significant enough to warrant recognition.[20] Courts have held that the "mere increased risk of identity theft

13. 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, and because the program was classified as a state secret, the plaintiffs did not and could not know for sure that they were being subjected to surveillance. *See* Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 757 (2016) (describing the government's strategy to avoid public judicial review of secret surveillance by combining secrecy with justiciability and standing).

14. *Clapper*, 568 U.S. at 414–15 n.5. In *Susan B. Anthony List v. Driehaus*, the Court, quoting *Clapper*, held that "[a]n 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).

15. 664 F.3d 38 (3d Cir. 2011).

16. *Id.* at 42.

17. *Id.*

18. *Id.* at 43.

19. *Id.* at 46.

20. *See, e.g.*, Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (holding that the increased risk of future identity theft or fraud stemming from a data breach was not sufficient to constitute imminent injury); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 363, 365–66 (M.D. Pa. 2015) (reasserting *Reilly* by agreeing that increasing the risk of identity theft does not suffice as injury); *In re* Horizon Healthcare Servs., Inc. Data Breach Litig., No. 13-7418 (CCC), 2015 WL 1472483, at *1, *5–6 (D.N.J. Mar. 31, 2015), *vacated*, 846 F.3d 625 (3d Cir. 2017) (holding that plaintiffs did not have standing in a case alleging imminent risk and harm of fraud stemming from the theft of several computers containing personal information that were held by defendants; plaintiffs were not able to show actual harm and could only speculate that future fraud may occur).

or identity fraud alone does not constitute a cognizable injury."[21] They have refused to find harm even in cases where hackers used malware to steal personal data and there was evidence of misuse of the data.[22] Claims have been summarily dismissed on the grounds that plaintiffs have not suffered identity theft or could not show an imminent threat of financial injury.[23]

Some courts, however, have pushed back against the trend and have found harm. The Sixth, Seventh, and Ninth Circuits have found standing for victims of data breaches based on the increased risk of identity theft.[24] In those cases, plaintiffs were found to have suffered actual, not hypothetical, injuries where hackers stole personal data from inadequately secured systems.[25] In *Remijas v. Neiman Marcus Group*, the Seventh Circuit reasoned, "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is,

21. Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *3 (E.D. La. May 4, 2015).

22. *E.g.*, Bradix v. Advance Stores Co., No. 16-4902, 2016 WL 3617717, *1–4 (E.D. La. July 6, 2016) (dismissing claims for lack of injury in fact in a case where the plaintiff alleged that one of defendant's employees gave employees' names, Social Security numbers, and gross wages to a hacker who used the information in unauthorized attempts to secure vehicle financing that appeared on the plaintiff's credit report because there was no proof that the attempts at fraud damaged the plaintiff's credit score); *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586, 2016 WL 81792 (D. Minn. Jan. 7, 2016) (finding no harm to support standing even though plaintiffs alleged that defendants released malicious software and disclosed payment card names and PINs because the only alleged misuse of personal data was a single unauthorized charge on one plaintiff's credit card).

23. *E.g.*, *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (declining to find standing where partial credit card numbers of 24 million customers were stolen because there were no allegations of misuse or unauthorized purchases); *Storm*, 90 F. Supp. 3d at 366 (finding no standing because the plaintiffs did not allege that they "actually suffered any form of identity theft as a result of the data breach," even though hackers had breached a payroll company's computer system and accessed confidential, personal information).

24. Galaria v. Nationwide Mut. Ins., 663 F. App'x 384, 385–86 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693–94 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014).

25. *See Galaria*, 663 F. App'x at 385–86 (holding that substantial risk of harm, coupled with reasonably incurred mitigation costs, supported standing in a data-breach case because theft of personal data by ill-intentioned criminals placed them at continuing, increased risk of fraud and identity theft and the plaintiff suffered three unauthorized attempts to open credit cards in his name); *Remijas*, 794 F.3d at 693–94 (holding that the plaintiffs had standing to sue in the wake of breach even though they had not experienced fraudulent charges on their credit cards because those plaintiffs knew from the fact that other plaintiffs' cards had been used fraudulently that their personal information had been stolen by individuals who intended to misuse it); *Krottner*, 628 F.3d at 1143 (holding increased risk of identity theft constituted an injury in fact where someone had attempted to open a bank account using stolen personal data because plaintiffs had alleged a "credible threat of real and immediate harm stemming from the theft of the laptop" with the unencrypted names, addresses, and Social Security numbers of 97,000 employees); *In re Target Corp.*, 66 F. Supp. 3d at 1157–59 (holding that unlawful charges, restricted or blocked access to bank accounts, inability to pay bills, and late payment charges or new card fees incurred by the plaintiffs constituted injuries in fact in the wake of the theft of credit card and personal data of 110 million customers).

sooner or later, to make fraudulent charges or assume those consumers' identities."[26] Courts have also held that plaintiffs faced a substantial risk of harm, sufficient to support standing, where the stolen data was posted on file-sharing websites for identity thieves.[27]

Despite these decisions, the weight of authority has leaned against finding harm. Data-breach lawsuits remained an area of unease, with courts struggling to develop a consistent and coherent approach. In data-breach cases, the nature of the injury has seemingly befuddled the courts.

In 2016, the U.S. Supreme Court in *Spokeo, Inc. v. Robins*[28] attempted to clarify the harm required for standing when injuries result from the mishandling of personal data. Yet far from providing guidance, the opinion fostered even more confusion about informational harms. In *Spokeo*, the plaintiff alleged that the defendant, a "people search engine," violated the federal Fair Credit Reporting Act (FCRA) when it published false information about him.[29] The defendant's dossier asserted that the plaintiff was wealthy, married with children, and worked in a professional field though he was none of those things.[30] The plaintiff alleged that the inaccuracies in the defendant's dossier damaged his employment chances by suggesting that he was overqualified and that he might be unwilling to relocate because of responsibilities to his nonexistent family.[31] The district court found that the plaintiff lacked standing to sue under Article III because the alleged injury—the defendant's publication of inaccurate information—was not an injury in fact.[32]

After the Ninth Circuit reinstated the plaintiff's case on the grounds that an inaccurate credit report, allegedly violating a statutory right, amounted to a particularized injury sufficient to support standing,[33] the Supreme Court granted the defendant's writ for certiorari.[34] In an opinion authored by Justice Alito, the Court instructed the Ninth Circuit to reconsider the standing question. The Court declared that the harm required for standing must be

---

26. *Remijas*, 794 F.3d at 693.

27. *E.g.*, Corona v. Sony Pictures Entm't, Inc., No. 14–CV–09600, 2015 WL 3916744, at *3 (C.D. Cal. June 15, 2017) (holding allegations that stolen data had been posted on file-sharing websites, alongside allegations that the data had been used by actors to send threatening emails, was "alone sufficient" to establish standing); *see also Galaria*, 663 F. App'x at 385–86 (finding standing where plaintiffs alleged, among other things, that an "illicit international market for stolen data" exists).

28. 136 S. Ct. 1540 (2016).

29. *Id.* at 1544.

30. *Id.* at 1546.

31. *Id.* at 1556 (Ginsburg, J., dissenting).

32. *Id.* at 1546 (majority opinion).

33. Robins v. Spokeo, Inc., 742 F.3d 409, 411–14 (9th Cir. 2014), *vacated* 136 S. Ct. 1540 (2016).

34. *Spokeo*, 136 S. Ct. at 1546.

"concrete," yet it suggested that "intangible harm," and even the "risk" of harm, could be sufficient to establish a concrete harm if intangible injury has a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[35]

The Court failed to elaborate on how all this added up. It said nothing about the relationship between the concreteness of harm and the need for at least a substantial risk of harm as discussed in *Clapper*. When will increased risk of injury constitute a "substantial risk of harm"? Why are some intangible injuries sufficient for standing while others are not? *Spokeo* did little to clear up the confusion about harms related to the mishandling of personal data.

Clapper and *Spokeo* have led to confusion about how harms involving personal data should be conceptualized. To many judges and policymakers, recognizing data-breach harms is akin to attempting to tap dance on quicksand, with the safest approach being to retreat to the safety of the most traditional notions of harm. Unfortunately, public conversation about data-breach harms rarely delves into the muddy conceptual waters. With some noted exceptions, scholarship has not given the issue sufficient attention.[36] Ryan Calo has thoughtfully laid out historical and conceptual support for treating anxiety as privacy harm.[37] In our view, anxiety and risk, together and alone, deserve recognition as compensable harms.

---

35. *Id.* at 1549.

36. Ryan Calo has done theoretically rich work on privacy harm, as has Paul Ohm. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011) [hereinafter *Boundaries*] (making the case that the boundaries of privacy harms can be distilled to objective harms and subjective harms); Ryan Calo, *Privacy Harm Exceptionalism*, 12 J. TELECOMM. & HIGH TECH. L. 361, 361, 364 (2014) [hereinafter *Exceptionalism*] (arguing that courts have required litigants to move mountains to prove harm resulting from privacy violations unlike countless other areas where redress is required for negative externalities imposed on individuals); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010) (asserting that privacy law is built around the mistaken principle that anonymized data cannot easily be "deanonymized" and that, accordingly, people are afforded much less privacy than they assume); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1196 (2015). Our previous work has tackled the issue as well. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 8–9 (2008) (introducing a new theory of privacy that abandons the traditional way of conceptualizing privacy); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1831 (2010) [hereinafter *Mainstreaming*] (contending that courts should invoke established tort remedies to address unwanted intrusions and disclosure of personal information instead of creating new privacy torts); 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, 243–45 (2007) [hereinafter *Reservoirs*].

37. Calo, *Boundaries*, *supra* note 35, at 1144–48; Calo, *Exceptionalism*, *supra* note 35, at 362–63. Calo argues that privacy harms have an objective component, which involves unanticipated or coerced use of personal information to an individual's disadvantage, and a subjective one, which involves the unwanted perception of observation. Calo, *Boundaries*, *supra* note 35, at 1144, 1148. Calo's framework recognizes anxiety suffered in the wake of a data breach as cognizable

This issue cries out for attention. The number of people affected by data breaches continues to rise as companies collect more and more personal data in inadequately secured data reservoirs.[38] Risk and anxiety are injuries in the here and now. Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage. Once victims learn about breaches, they may be chilled from engaging in activities that depend on good credit, like house- and job-hunting. Data-breach victims might decline to search for a new home or employment since there is an increased chance that lenders or employers will find their credit reports marred by theft.[39] They face an increased chance of being preyed upon by blackmailers, extortionists, and fraudsters promising quick fixes in exchange for data or money.[40] Emotional distress is a crucial aspect of the suffering. Knowing that thieves may be using one's personal data for criminal ends can produce significant anxiety. Because companies do not have to internalize these negative externalities borne by individuals, the number of data breaches continues to grow.[41] Data breaches have become an epic problem.

In this Article, we focus on data-breach harms. We explore why courts have struggled with the issue, and we offer an approach to address data-breach harms that has roots in existing law. In what follows, we explore the nature of data-breach harms and demonstrate how the law is far from closed off to recognizing them. We show that there are ample conceptual foundations in the law to address risk and anxiety and thus to recognize data-breach harms. In some areas, the law has been developing gingerly in the direction of recognizing concepts helpful to recognizing data-breach harms;

(subjective) harm, but does not recognize increased risk of identity theft and fraud as a cognizable (objective) harm. *Id.* at 1156.

38. *See* Lily Hay Newman, *If You Want to Stop Big Data Breaches, Start with Databases*, WIRED (Mar. 29, 2017), https://www.wired.com/2017/03/want-stop-big-data-breaches-start-databases/ [https://perma.cc/7WS2-MVEB] (observing that data breaches often result from databases "with outdated and weak default security configurations"); *At Mid-Year, U.S. Data Breaches Increase at Record Pace*, IDENTITY THEFT RESOURCE CTR. (July 18, 2017), http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release [https://perma.cc/3F9H-CZV2] (reporting that in the first half of 2017, data breaches reached a half-year record high).

39. *See* Ron Lieber, *Why the Equifax Breach Stings So Bad*, N.Y. TIMES (Sept. 22, 2017), https://www.nytimes.com/2017/09/22/your-money/equifax-breach.html [https://perma.cc/AQ57-REQA] (stating that home loan officers and employers check credit scores and bad credit scores will likely yield rejections from both).

40. Sarah Perez, *Scammers Now Targeting Anthem Data Breach Victims Via Email and Phone*, TECHCRUNCH (Feb. 9, 2015), https://techcrunch.com/2015/02/09/scammers-now-targeting-anthem-data-breach-victims-via-email-and-phone/ [https://perma.cc/3Q3V-8XL9].

41. *See* IDENTITY THEFT RESOURCE CTR., *supra* note 38 (reporting on the record increase in data breaches in recent years); Benjamin Dean, *Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity*, QUARTZ (Mar. 5, 2015), https://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/ [https://perma.cc/6BH7-Z4GW] (arguing that private companies lack incentive to invest in information security because other parties typically bear the costs resulting from data breaches).

in other areas of the law, such concepts are widely accepted yet remain sequestered from similar kinds of harm in other contexts.

The past century has witnessed great advances in how the law deals with risk and anxiety. Risk is readily addressed, quantified, and factored into business decisions. Despite this progress, many courts in data-breach cases seem to freeze in the headlights and find risk too difficult to assess. Ironically, the very companies being sued for data breaches make high-stakes decisions about cyber security based upon an analysis of risk. Indeed, in areas of law beyond data-breach cases, courts have developed robust and concrete understandings of risk.[42] Sufficient foundations in law exist for courts to assess increased risk of harm in data-breach cases.

Anxiety is also readily dismissed on the grounds that it is too speculative and insubstantial to serve as a basis of cognizable harm in data-breach cases.[43] In other contexts, however, courts routinely accept various forms of emotional distress, including anxiety, as sufficient harm.[44] Indeed, in some areas, the issue of harm is not even discussed in most cases and is rarely an issue on appeal.[45] For example, the privacy torts, recognized in the vast majority of states, allow plaintiffs to recover for the disclosure of private information or the improper intrusion into private matters resulting in emotional distress if the defendant's conduct is "highly offensive to the reasonable person."[46] The tort of breach of confidentiality recognizes emotional distress as a cognizable injury without the need to show highly offensive conduct.[47]

If a news media site published a nude photo or sex video of a person without consent, the plaintiff could prevail without establishing financial losses or physical injury because the gravamen of the harm is emotional distress.[48] Recently, the famous former pro wrester Hulk Hogan won $115 million in compensatory damages from media site Gawker for posting a sex video involving him without his consent. In cases involving data breaches or improper sharing of data, however, claims of emotional distress are dismissed as insufficient without even a whisper of the extensive body of law under the privacy torts that establishes otherwise. Why does the embarrassment over a sex video amount to $115 million worth of harm but the anxiety over the loss

42. *See infra* section II(A)(2).

43. Dana Post, *Plaintiffs Alleging Only "Future Harm" Following a Data Breach Continue to Face a High Bar*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 28, 2014), https://iapp.org/news/a/plaintiffs-alleging-only-future-harm-following-a-data-breach-continue-to-fa/ [https://perma.cc/PX7K-KHZH].

44. *See infra* section II(B)(2).

45. *See* cases cited *infra* notes 181–93.

46. Citron, *Mainstreaming*, *supra* note 36, at 1827.

47. DAVID A. ELDER, PRIVACY TORTS § 3:8 (2002).

48. *See infra* section II(B)(2).

of personal data (such as a Social Security number and financial information) amount to no harm?

This Article has three parts: In Part I, we discuss the way that courts are currently deciding cases involving data-breach harms. In Part II, we explore why the law struggles with recognizing privacy and security violations as having caused cognizable harm. In Part III, we demonstrate that there are foundations in the law for a coherent recognition of harm based upon increased risk and anxiety. We build on this foundation, offering a framework for courts to assess risk and anxiety in a principled and consistent way.

I. The Emerging Law of Data-Breach Harms

Harm is indispensable to most private law claims. Generally speaking, harm is understood as the impairment, or setback, of a person, entity, or society's interests.[49] People or entities suffer harm if they are in worse shape than they would be in had the activity not occurred.[50] Harm frustrates a person's ability to "fashion a life . . . that is distinctively and authentically hers."[51] Harm can involve the impairment of a person's interest in physical integrity, "intellectual acuity, emotional stability, the absence of groundless anxieties and resentments, the capacity to engage normally in social intercourse . . . a tolerable social and physical environment, and a certain amount of freedom from interference and coercion."[52]

A legally cognizable harm is harm that the law recognizes as worthy of redress, deterrence, or punishment.[53] Reasonable foreseeability of harm is a fundamental principle of much of private law.[54] Plaintiffs must prove harm even if the defendant indisputably acted wrongly and violated the law. In tort suits, plaintiffs must prove that they were injured by the defendant's actions. In *The Common Law*, Oliver Wendell Holmes identified harm as the evil

---

49. JOEL FEINBERG, HARM TO OTHERS: THE MORAL LIMITS OF CRIMINAL LAW 34 (1984) (explaining that harm involves the thwarting, setting back, or defeating of a person or entity's interest). Competing accounts of harm argue that harm involves events that are bad to suffer or impose conditions that impair agency. *Id*.

50. JOEL FEINBERG, *Wrongful Life and the Counterfactual Element in Harming*, *in* FREEDOM & FULFILLMENT: PHILOSOPHICAL ESSAYS 3, 4 (1992); *see* Stephen Perry, *Harm, History, and Counterfactuals*, 40 SAN DIEGO L. REV. 1283, 1292 (2003) (exploring a concept of harm as a "historical worsening," which may involve a subsequent counterfactual analysis).

51. Seana Valentine Shiffrin, *Wrongful Life, Procreative Responsibility, and the Significance of Harm*, 5 LEGAL THEORY 117, 123–24 (1999).

52. FEINBERG, *supra* note 49, at 37.

53. As Joel Feinberg explains, harms may involve invasions or setbacks to interests but not all invasions of interests are worthy of law's attention. FEINBERG, *supra* note 48, at 34–35. Law may ignore the wrongful behavior causing harm because the defendant acted justifiably or the targeted individual had no right to expect that his interests be protected. *Id.*

54. Gregory C. Keating, *When is Emotional Distress Harm?*, *in* TORT LAW: CHALLENGING ORTHODOXY 273, 273 (Stephen G.A. Pitel et al. eds., 2013).

against which tort law was directed.[55] Regardless of whether the defendant acted negligently, recklessly, or intentionally—no matter how wrongful the defendant's conduct may have been—if harm is not proven, then plaintiffs cannot obtain relief.[56] To be sure, legislation sometimes permits statutory damages or includes liquidated damages provisions, which permit redress without additional showings of harm.[57] The harm is understood as the interference with the right recognized in the statute, so long as the plaintiff has suffered some setback to tangible or intangible interests.[58]

Beyond the substance of private law claims, federal courts require that plaintiffs have standing to bring suit in accord with Article III of the U.S. Constitution. Standing doctrine requires that plaintiffs allege an injury in fact.[59] The injury must be concrete, particularized, and "actual or imminent, not conjectural or hypothetical."[60] If a plaintiff lacks standing to bring a claim, a federal court cannot hear it.[61]

Although the requirements for standing and substantive causes of action are different, the issue of harm that undergirds both is strikingly similar. In most cases, the way courts think about harm for standing is nearly identical to the way courts approach harm in substantive claims. We focus on harm because it is central to the jurisprudence of private law claims.

No matter whether harm is raised for the purposes of standing or determining the cognizability of private claims, harm drives the way courts

---

55. *See* OLIVER WENDELL HOLMES, THE COMMON LAW 64 (Mark DeWolfe Howe ed., 1963) ("The business of the law of torts is to fix the dividing lines between those cases in which a man is liable for harm which he has done, and those in which he is not."); *see also* Thomas C. Grey, *Accidental Torts*, 54 VAND. L. REV. 1225, 1272 (2001) (exploring Holmes's harm-based approach).

56. In certain circumstances, there may be distinct criminal laws and regulatory enforcement that would punish the defendant. In the absence of such penalties, the defendant can engage in the wrongdoing and violate the law without suffering any penalty.

57. Copyright law is a prime example of statutory damages without harm. *See* 17 U.S.C. § 504(c)(1) (2012) (stating that the copyright owner may at any time before a final judgment recover "an award of statutory damages for all infringements involved in the action" instead of "actual damages and profits").

58. *See* Spokeo v. Robins, 136 S. Ct. 1540, 1549 (2016) (explaining that concrete injuries may be both tangible and intangible, and that "[i]n determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles"). Some statutes like the Privacy Act of 1974 require an additional showing of harm for individuals to bring suit. *See* NASA v. Nelson, 131 S. Ct. 746, 763 (2011) (rejecting a claim under the act where plaintiffs alleged only a possibility of harm). Similarly, some state Unfair and Deceptive Practice acts (UDPA) permit consumers to seek compensation for losses caused by unfair and deceptive commercial practices only if those practices result in injury. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 798 (2016) ("[P]rivate UDAP claims are routinely dismissed due to a lack of an 'injury in fact' sufficient to support a finding of standing or cognizable harms, or due to the economic loss rule."). Because private UDAP claims require a showing of harm—whether or not statutes so require—courts routinely dismiss them.

59. Friends of the Earth Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180 (2000).

60. *Id.*

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

think about data-breach cases, most often resulting in their dismissal early in the litigation. Courts have found a lack of injury in fact to support standing or have concluded that there is no harm caused by various torts or other causes of action. In this Part, we examine how courts have conceptualized harm in their rejection of these claims.

A. Judicial Approaches to Data-Breach Harms

Data breaches usually involve various types of personal data, such as financial account information, driver's license numbers, biometric markers, and Social Security numbers. The Office of Policy Management (OPM) breach leaked people's fingerprints, background check information, and analyses of security risks.[62] The Ashley Madison breach released information about people's extramarital affairs.[63] The Sony breach involved employee email.[64] The Target breach resulted in the leaking of credit card information, bank account numbers, and other financial data.[65] Other breaches result in the disclosure of passwords, children's information, location data, and medical records.

Plaintiffs in data-breach cases have pursued a number of causes of action, including negligence, privacy torts, and breach of fiduciary duty.[66] Other claims assert violations of state unfair and deceptive commercial acts and practice statutes (UDAP laws), state data security laws, the federal Privacy Act, and the federal Fair Credit Reporting Act (FCRA).[67] In a study of 230 data-breach lawsuits between 2004 and 2014, plaintiffs brought more than eighty-six different causes of action.[68]

---

62. Kim Zetter, *The Massive OPM Hack Actually Hit 21 Million People*, WIRED (July 9, 2015), http://www.wired.com/2015/07/massive-opm-hack-actually-affected-25-million/ [https://perma.cc/CK7S-EWBA]; Kim Zetter & Andy Greenberg, *Why OPM Is A Security and Privacy Debacle*, WIRED (June 11, 2015) http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/ [https://perma.cc/PUB3-QJHS].

63. Danielle Keats Citron & Maram Salaheldin, *Leave the Cheaters in Peace: If You Poke Around the Ashley Madison Data, You're Aiding and Abetting the Hackers*, N.Y. DAILY NEWS (Aug. 24, 2015), http://www.nydailynews.com/opinion/citron-salaheldin-leave-cheaters-peace-article-1.2333852 [https://perma.cc/2R76-F69Y].

64. Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know/ [https://perma.cc/9K6N-SJKE].

65. Jim Finkle & David Henry, *Exclusive: Target Hackers Stole Encrypted Bank PINs - Source*, REUTERS (Dec. 24, 2013), https://www.reuters.com/article/us-target-databreach/exclusive-target-hackers-stole-encrypted-bank-pins-source-idUSBRE9BN0L220131225 [https://perma.cc/G3VZ-6RX2]; Kim Zetter, *Target Admits Massive Credit Card Breach; 40 Million Affected*, WIRED (Dec. 19, 2013), https://www.wired.com/2013/12/target-hack-hits-40-million/ [https://perma.cc/C6CJ-DY26].

66. Romanosky et al., *supra* note 2, at 100, 101 fig.7.

67. *Id.*

68. *Id.* at 102.

Data-breach cases are often filed in federal court or removed from state court under the federal Class Action Fairness Act (CAFA).[69] Under CAFA, class actions can be removed to federal court for state-law claims exceeding $5 million where at least one member of the putative class and one defendant reside in different states.[70] At the federal level, harm thus must often be established twice—first to make it past the hurdle of standing and second to satisfy the elements of various causes of action.

Although plaintiffs advance a number of theories of harm, at bottom, their claims are based on three overarching theories: (1) data breaches create a risk of future injury, (2) plaintiffs take preventative measures to reduce the risk of injury, and (3) plaintiffs experience anxiety as a result of data breaches compromising their personal data.

1. Risk of Future Injury.—A common theory advanced by plaintiffs is that a data breach has increased their risk of future identity theft or fraud. The majority of courts reject that theory of harm. Plaintiffs' increased risk of identity theft is regarded as too speculative a harm even in cases where thieves allegedly stole personal data.[71] Courts view the increased risk of identity theft not as an "actual injury" but rather as "speculation of future harm."[72]

The trend is that if a person's personal data has not yet been used to commit identity theft or fraud, then courts find that plaintiffs have suffered no harm.[73] In a case where plaintiffs' sensitive financial data was accessed

69. Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) (2012).

70. *Id.* § 1332(d)(2)(A).

71. *See, e.g.*, Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006) (granting the defendant's motion for summary judgment in a case involving the theft of personal data from the defendant's system because there was no indication that the information on the stolen computers had been misused); Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *6 (D. Minn. Feb. 7, 2006) (holding that the plaintiff did not raise a genuine issue of material fact on injury because there was no evidence that the thieves accessed the allegedly stolen data).

72. *E.g.*, *In re* Barnes & Noble Pin Pad Litig., No. 12–cv–8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) (dismissing a claim of harm based on increased risk of identity theft as speculation of future harm); Hammer v. Sam's East, Inc., No. 12–cv–2618–CM, 2013 WL 3746573, at *3 (D. Kan. July 16, 2013) ("[N]o court has found that a mere increased risk of identity theft or fraud constitutes an injury in fact for standing purposes without some alleged theft of personal data or security breach.").

73. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding that plaintiffs do not suffer harm until their information is misused); Hammond v. Bank of N.Y., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (holding that plaintiffs lacked standing because they did not produce evidence to suggest their injuries were more than speculative); Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (dismissing the plaintiff's negligence claim in a case in which the defendant's databases that stored the plaintiff's personal data was hacked because being at a higher risk for fraud is insufficient harm to warrant standing).

by unknown third parties, a federal district court dismissed the class suit alleging increased risk of identity fraud because plaintiffs' "credit information and bank accounts look[ed] the same today as they did" before the breach.[74] Because hackers had not opened new bank accounts or credit cards in plaintiffs' names, there was no harm.[75] This was true in *Key v. DSW Inc.*,[76] where thieves gained access to the defendant shoe retailer's computer system containing the financial data of 96,000 customers.[77] The court found no harm because plaintiffs only alleged the possibility of being victimized "at some unidentified point in the indefinite future."[78]

For some courts, there are simply too many contingencies at play, including the varied skills and intent of third-party hackers, to warrant a finding of harm.[79] In *Fernandez v. Leidos, Inc.*,[80] for instance, the district court dismissed the plaintiff's increased risk of harm in the wake of theft of backup tapes with his personal data because the capabilities and criminal intentions of the data thieves were speculative.[81]

Even when plaintiffs quantify the extent to which the data breach has elevated their risk of future harm, courts still find the harm too speculative to proceed.[82] In *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*,[83] the plaintiffs argued that they were nearly ten times more likely to be victims of identity theft.[84] The court found that the "degree by which the risk of harm has increased [wa]s irrelevant" because it failed to suggest that the harm was "certainly impending."[85] Another court sharpened the point, reasoning that identity theft was unlikely to happen in

74. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015).

75. *Id.*

76. 454 F. Supp. 2d 684 (S.D. Ohio 2006).

77. *Id.* at 685–86.

78. *Id.* at 690.

79. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011) ("Any damages that may occur [in data-breach cases with no allegations of misuse] are entirely speculative and dependent on the skill and intent of the hacker." (citation omitted)); Stapleton v. Tampa Bay Surgery Ctr., Inc., No. 8:17-cv-1540-T-30AEP, 2017 WL 3732102, at *3 (M.D. Fla. Aug. 30, 2017) ("While Plaintiffs argue that the mere fact that there was data breach is sufficient to constitute imminent injury, the Court cannot agree with that sort of *ipse dixit* reasoning. Something more than the mere data breach must be alleged before Plaintiffs can show they have a substantial risk of injury.").

80. 127 F. Supp. 3d 1078 (E.D. Cal. 2015).

81. *Id.* at 1086–88.

82. *E.g.*, Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366–67 (M.D. Pa. 2015) (rejecting an increased risk of identity theft as a basis for injury "[e]ven though Plaintiffs may indeed be at greater risk of identity theft" because plaintiffs did not "allege that any of them [had] become actual victims of identity theft"); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("[I]ncreased risk of harm alone does not constitute an injury in fact.").

83. 45 F. Supp. 3d 14 (D.D.C. 2014).

84. *Id.* at 25.

85. *Id.*

the future since the plaintiffs had not experienced fraud in the year after the breach.[86]

Although three Courts of Appeals have recognized increased risk of harm as cognizable, their cases involved allegations about the malicious purpose of hackers or actual or attempted misuses of leaked personal data.[87] In *Remijas*, the Seventh Circuit found the risk of harm "immediate and very real" because the data "was in the hands of hackers who used malware to breach the defendant's systems," and "fraudulent charges had shown up on the credit cards of some of its customers."[88] Moreover, the defendant "contacted members of the class to tell them they were at risk," which the court viewed as an admission that the plaintiffs had suffered nonspeculative harm.[89] In *Krottner v. Starbucks Corp.*,[90] the Ninth Circuit conferred standing on the plaintiffs because there was a subsequent attempt to open a bank account with personal data following the theft of a laptop.[91]

In most cases, however, increased risk of future injury fails as a theory of cognizable harm. The motives of those who obtained the data are unknown, and the plaintiffs have not yet suffered identity theft or other forms of financial fraud. It will not be clear who has the data or what they will do with it. Proving that the risk of harm is "certainly impending" is challenging because the harm from a data breach is not immediate. Even in many cases where hackers accessed personal data and their malicious motive can be inferred, courts have still refused to find harm.[92]

---

86. *Storm*, 90 F. Supp. 3d at 366–67.

87. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (holding an "increased risk of fraudulent charges and identity theft" constituted an injury "concrete enough to support a lawsuit" because the data had already been stolen); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015) ("[I]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010) (holding an allegation of increased risk of identity theft was sufficient to confer standing when plaintiffs alleged a specific instance of an attempt to use stolen information to open a bank account).

88. *Remijas*, 794 F.3d at 690, 693; *see also* Danielle Citron, *Some Good News for Data Breach Victims, for a Change*, FORBES (July 21, 2015), http://www.forbes.com/sites/daniellecitron/2015/07/21/some-good-news-for-data-breach-victims-for-a-change/ [https://perma.cc/DS3K-WY86] (explaining the significance of the *Remijas* court's injury-in-fact holding).

89. *Remijas*, 794 F.3d at 696; *accord Lewert*, 819 F.3d at 967 (finding credence in the risk of identity theft alleged by plaintiffs because the defendant had encouraged customers whose data had been stolen to monitor their credit reports). The Sixth Circuit's recent *Galaria* decision similarly pointed to the defendant's provision of credit monitoring as supporting increased risk of harm. Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388–89 (6th Cir. 2016).

90. 628 F.3d 1139 (9th Cir. 2010).

91. *Id.* at 1142–43.

92. *See, e.g.*, Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1019, 1021 (D. Minn. 2006) (finding "no present injury or reasonably certain future injury to support damages for any alleged increased risk or harm" after theft of computers containing unencrypted customer information,

2. Preventative Measures to Protect Against Future Injury.—A related theory based on future risk of injury is that plaintiffs incur out-of-pocket costs to mitigate the risk of identity theft or fraud. They spend time and money placing alerts with credit reporting agencies and subscribing to identity-theft protection and credit-monitoring services. They devote time and money to monitor various accounts and go through the hassle of changing service providers to prevent further breaches. Plaintiffs contend that the cost of these measures presents a specific monetary value that can be associated with the improper exposure of personal data. Courts, however, often reject this theory of harm, viewing plaintiffs' expenses as attempts to "manufacture" injury.[93]

The preventative-measure theory of harm typically fails because it is based upon the increased-risk-of-future-injury theory.[94] The concern of courts is that any plaintiff could find some measure to spend money to mitigate any risk. Said another way, monetary expenditures are viewed as too easy to manufacture. If such expenses were recognized as a cognizable injury, plaintiffs' lawyers would just instruct their clients to spend time and money on mitigation measures to create harm. Having rejected the risk of future injury, courts reject the expenditure of time and money in the present to turn the risk of future injury into more cognizable monetary losses.

3. Anxiety.—Plaintiffs have argued that data breaches caused them emotional distress (in particular, anxiety), but courts have rejected these claims nearly every time. As a federal district court in New Jersey noted, "[c]ourts across the country have rejected 'emotional distress' as a basis for" finding harm because plaintiffs' fear of identity theft or fraud is based on speculative conclusions that personal data will be used in a malicious way.[95]

According to one court, "[p]laintiffs' bald assertion of 'emotional distress including anxiety, fear of being victimized, harassment and embarrassment' is unexplained by any facts at all, let alone facts plausibly

---

including names, addresses, Social Security numbers, and account numbers); *see also* cases cited *supra* notes 71–86.

93. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013) ("We hold that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."); Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 470–71 (D.N.J. 2013) ("Plaintiff's decision to [incur expenses] was based entirely on her speculative belief . . . . Therefore, her assertion is one that claims injury for expenses incurred in anticipation of future harm, and is not sufficient for purposes of establishing Article III standing.").

94. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) ("[T]hey prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent. The claim that they incurred expenses in anticipation of future harm, therefore, is not sufficient to confer standing.").

95. Crisafulli v. Ameritas Life Ins., No. 13–5937, 2015 WL 1969176, at *4 (D.N.J. Apr. 30, 2015).

suggesting emotional injury."[96] One court stated, "even if [the risk of identity theft] is enough to engender some anxiety" and, "even if their fears are rational," plaintiffs lacked standing "based on risk alone."[97] As another court concluded: "Emotional distress in the wake of a security breach is insufficient to establish standing . . . ."[98] Unless there is an "imminent threat" of personal data being used in a "malicious way," plaintiffs' anxiety and emotional suffering are viewed as insufficient to constitute harm.[99] Most courts consider plaintiffs' fear, anxiety, and psychic distress about their increased risk of identity theft and other abuses too remote to warrant recognition.[100]

B. Cramped View of Harm: Visceral and Vested

As the previous section has shown, cases are dismissed for lack of harm even when a company's negligence has clearly caused a data breach. Even in the face of wrongful conduct by defendants, courts are denying plaintiffs redress. The reason is because courts view the harm in overly narrow ways. Courts insist that data-breach harms be visceral—easy to see, measure, and quantify.[101] They require harms to be vested—already materialized in the here and now. Plaintiffs must experience physical, monetary, or property damage or, at least, the damage must be imminent.[102]

This cramped understanding of harm harkens back to early conceptions of the common law. Nineteenth-century tort claims required proof of physical injury or property loss.[103] Financial losses could be recovered in tort actions if defendants owed plaintiffs a special duty of care.[104] Along these lines,

---

96. *Id.*

97. *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014); *see also* Maglio v. Advocate Health & Hosps. Corp., 40 N.E.3d 746, 755 (Ill. App. 2015) (suggesting that "speculative and conclusory" allegations of possible "anxiety and emotional distress" caused by data breaches do not give rise to standing).

98. *In re* Barnes & Noble Pin Pad Litig., No. 12–cv–8617, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013).

99. *Id.*

100. Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009).

101. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011) (emphasizing that a "quantifiable [rather than speculative] risk of damage" is necessary to establish data harm).

102. *See, e.g.*, *Amburgy*, 671 F. Supp. 2d at 1050, 1053–55 (asserting that the "injury or threat of injury must be concrete and particularized, actual and imminent; not conjectural or hypothetical").

103. Gregory C. Keating, *The Priority of Respect Over Repair*, 18 LEGAL THEORY J. 293, 332 & n.97 (2012).

104. *See* John A. Fisher, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 237–38 ("[T]he Economic Loss Rule operates to preclude recovery when the parties have a direct contractual relationship and damages are consequential (lost profits), rather than direct (property damage or personal injury)."). The economic loss rule does not apply when a defendant owes the plaintiffs a special duty of care. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1173–76 (D. Minn.

courts have recognized claims for privacy violations only where redress is sought for tangible financial losses.[105] Courts have found sufficient injury in data-breach cases where the exposure of personal data has led to identity theft.[106] But without proof of physical harm or financial loss, courts rarely recognize harm.[107]

Requiring harm to be visceral and vested has severely restricted the recognition of data-breach harms, which rarely have these qualities. Data-breach harms are not easy to see, at least not in any physical way. They are not tangible like broken limbs and destroyed property. Instead, the harm is intangible. Data breaches increase a person's risk of identity theft or fraud and cause emotional distress as a result of that risk.

Despite the intangible nature of these injuries, data breaches inflict real compensable injuries. Data breaches raise significant public concern and generate legislative activity.[108] Would all this concern and activity exist if there were no harm? Why would more than 90% of the states pass data-breach-notification laws in the past decade if breaches did not cause harm?[109] Why would the Federal Trade Commission and state attorneys general

---

2014) (discussing special-relationship and independent-duty exceptions to the economic loss rule, allowing recovery of financial losses in tort).

105. *E.g.*, Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 800 (N.D. Cal. 2011) (finding a recoverable injury where the alleged privacy violation had deprived plaintiffs of the measurable, concrete financial value of their endorsement for advertising purposes); *In re* Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588, at *6 (N.D. Ill. Sept. 3, 2013) (noting that a fraudulent charge resulting from a private data breach would only create a cognizable injury if the charge was unreimbursed).

106. *E.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1330 (11th Cir. 2012); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 696–97 (7th Cir. 2015). It can, however, be difficult to pinpoint a single actor for the harm suffered in the wake of a data breach. There are many participants that contribute to the harm experience by identity-theft victims: the entities that leaked the data, the companies that allowed thieves to open up accounts in victims' names, and the credit reporting agencies that assembled the faulty information and use it to report on people's reputations. *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1260–61 (2003) (assigning blame for identity theft to a broad group of private and governmental actors in addition to the thieves). When victims attempt to clean up their credit reports, they are often prevented from doing so by uncooperative credit-reporting agencies and creditors. Tara Siegel Bernard, *TransUnion, Equifax and Experian Agree to Overhaul Credit Reporting Practices*, N.Y. TIMES (March 9, 2015), http://www.nytimes.com/2015/03/10/business/big-credit-reporting-agencies-to-overhaul-error-fixing-process.html?_r=0 [https://perma.cc/6Q5V-3QY2].

107. *E.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 496 (Me. 2010) (holding that reasonable time and effort spent to mitigate possible future losses was not a cognizable harm in tort or implied contract).

108. *See* Daniel R. Stoller, *Massive Equifax Cyberattack May Push Congress on Breach Notice Law*, BLOOMBERG BNA (Sept. 8, 2017), https://www.bna.com/massive-equifax-cyberattack-n57982087651/ [https://perma.cc/8U9D-M62D] (anticipating strong legislative response to the Equifax data breach based on past data-breach responses).

109. *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/K3U2-UBB2].

expend considerable time and resources pursuing data-breach cases?[110] In short, if data breaches cause no harm, then why do federal and state law-enforcement agencies devote resources to addressing them?

Data-breach harms might be akin to invisible objects in the middle of a crowded room. We may not be able to see an invisible object, but we see how everyone is bumping into it, how they are changing where they stand because of it, how they are walking different routes to avoid it, and so on. The object is invisible to the naked eye, but it is having a significant effect and people are expending a lot of time and energy to deal with it. To understand its impact, the best approach is not to look directly at it. Instead, we need to look at the activity generated by it and around it. The same is true with data-breach harms. When data-breach harms are studied in isolation, the real harm can be difficult to see. As with the invisible object, one must step back and observe the reactions to the data breach.

As we explore in Part II, in other areas of the law, conceptions of harm have evolved to recognize injury that is hard to see or measure. This is true for pain and suffering, loss of consortium, and other matters that are not easily translated into monetary terms. This is true for emotional distress and risk-oriented injuries. Law has developed ways to arrive at dollar figures for these harms, and it should evolve to do so in the context of data-breach harms.

II. Risk and Anxiety as Harms

The nature of data-breach harms is a complex issue that courts have given far too little attention. In this Part, we explore why courts have struggled with risk and anxiety, the key dimensions to data-breach harms. We contend that these harms are far from fanciful or trivial. Data-breach harms are real, and compelling reasons exist for recognizing them. In this Part, we demonstrate that contrary to findings that no legal basis exists to recognize harm arising out of data breaches, there is a substantial basis in legal doctrine to recognize data-breach harms. These precedents involve other bodies of law, some closely related to the law of data breaches. Rather than ignoring these legal foundations for recognizing harm, courts should build upon them. Doing so would ensure conceptual coherence to the judiciary's approach. Moreover, the existence of these other areas of law that recognize similar types of harm demonstrates that data-breach harms can be recognized without causing calamity in the law.

A. Risk as Harm

1. Understanding Risk.—In data-breach cases, courts have difficulty with the concept of risk. A problem is that fraud may not surface until after

110. *See* Citron, *State Attorneys General*, *supra* note 58, at 748–49, 755.

an identity thief combines leaked personal data with other information. Because the downstream use of improperly obtained personal data is not known at the time of the breach and because it depends upon the aggregation of disparate sources of personal data, courts have difficulty conceptualizing the harm.

What does that risk entail? It may take months or years before leaked personal data is abused, but when it happens, the harm can be profound. Identity-theft victims may face financial ruin. Identity thieves may plunder victims' credit, riddling victims' credit reports with false information including debts and second mortgages obtained in victims' names. Victims struggling with identity theft may be forced to file for bankruptcy, and some may lose their homes.[111] Victims may be turned down for loans or end up paying higher interest rates on credit cards.[112] Their utilities may be cut off and their services denied.[113] Victims' stolen health information may be used to obtain medical care, saddling them with hefty hospital bills and a thief's treatment records.[114] Victims may incur legal fees and have to cover bounced checks. In 2012, the average cost of repairing identity theft was $1,769, and the median loss was $300.[115] On average, it takes up to thirty hours to resolve problems when identity thieves open new accounts in victims' names.[116] To be sure, some types of data-breach harms are more quickly realized. Payment-card fraud, for example, usually occurs shortly after payment-card data is compromised. Because card numbers get cancelled quickly, fraudsters act very fast.[117]

As Michael Sussmann, a lawyer in Perkins Coie's privacy and data security practice, explains: "The data is sold off, and it could be a while before it's used. . . . There's often a very big delay before having a loss."[118] Similarly, Ed Mierzwinski, the federal Consumer Program Director and senior fellow for U.S. PIRG, notes:

---

111. J. Craig Anderson, *Identity Theft Growing, Costly to Victims*, USA TODAY (Apr. 14, 2013), http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/ [https://perma.cc/7T5Q-DTHH].

112. BUREAU OF JUST. STAT., U.S. DEP'T OF JUST., NCJ 243779, VICTIMS OF IDENTITY THEFT, 2012, at 7 (2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf [https://perma.cc/773U-SHVT].

113. *Id.*

114. Thomas Clifford, Note, *Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?*, NW. J.L. & SOC. POL'Y, Fall 2016, at 45, 45.

115. BUREAU OF JUST. STAT., *supra* note 112, at 6.

116. *Id.* at 10.

117. *See* Andrea Peterson, *Data Exposed in Breaches Can Follow People Forever. The Protections Offered in Their Wake Don't.*, WASH. POST (June 15, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/06/15/data-exposed-in-breaches-can-follow-people-forever-the-protections-offered-in-their-wake-dont/ [https://perma.cc/JBF5-4K6X] (explaining that card providers quickly identify and replace at-risk card numbers).

118. *Id.*

> Credit card numbers and debit card numbers have a short shelf life, because banks figure out which cards are at risk, and people get new numbers without asking for them[.] Social Security [n]umbers have a very long shelf life—a bad guy that's smart won't use it immediately, he'll keep a hoard of numbers and use them in a couple of years.[119]

Harm may occur well beyond the statute of limitations, and the timing of the harm might be different for each victim.

The problem with identity theft is that personal data cannot readily be "cancelled" like a credit-card number. Social Security numbers are difficult to change. Other personal data such as birth date and mother's maiden name cannot be replaced. Biometric data such as fingerprints or eye scans, health information, and genetic data cannot be exchanged. A criminal may obtain a victim's personal data and use it months or years later; the data will still be useful for committing fraud.

Another challenge for assessing data-breach harms is the great difficulty in catching identity thieves. Without information about where an identity thief obtained the data, a plaintiff will have difficulty linking the harm to a particular data breach or data disclosure.[120] Ironically, the very factors that make identity theft so harmful—the difficulty in catching the perpetrators and the fact that it can continue indefinitely—are what impede victims' ability to obtain redress in the courts.

What of the argument that "[a] risk of privacy harm is no more a privacy harm than a chance of a burn is a burn"?[121] Unlike the chance of a burn while cooking in the kitchen, the risk of harm after a data breach inflicts harm in the here and now. To start, data-breach victims incur expenses to mitigate the damage. Data-breach victims incur out-of-pocket costs to minimize future losses. They purchase identity-theft-protection services and insurance to minimize the impact of fraud.[122] Their opportunity costs are real. Individuals spend time monitoring their accounts, which pulls them away from their jobs. In cases involving privacy violations and inadequate data security, consumers bear the lion's share of these costs because courts view them as too attenuated to recognize as harm.

---

119. *Id.*

120. Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 116 (Anupam Chander et al. eds., 2008).

121. Calo, *Boundaries*, *supra* note 36, at 1157.

122. *See* Press Release, Accenture, One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals (Feb. 20, 2017), https://newsroom.accenture.com/news/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm [https://perma.cc/2U3Q-HAP3] (detailing a survey of consumers which found nearly all data-breach victims took some type of action in response to a breach, such as purchasing insurance plans or subscribing to identity-protection services).

It is rational to spend time and money to mitigate the possibility of harm in the future. Insurance exists for this very purpose. There are numerous products and services aimed at risk mitigation. Indeed, after data breaches, organizations often offer affected individuals free credit monitoring.[123] State attorneys general often insist that companies pay consumers one to two years of credit monitoring and identity-theft insurance after a security breach.[124]

Another component of the data-breach harm involves a chilling of a person's ability to engage in life's important activities. As a result of a data breach, a person's increased risk of identity theft might prevent her from buying a new house. Identity theft, when it occurs, pollutes a person's credit report, making it difficult if not impossible to obtain a loan. In the face of a greater risk of identity theft, a person might be reluctant to take the steps necessary to buy a home, such as placing an existing home on the market, going house hunting, and making an offer with a deposit. Why take those expensive and time-consuming steps if there is a chance that her credit report might be damaged and thus jeopardize her deposit on a home? Why sell one's current home if one would be unable to buy a new one due to a marred credit report? Credit reports take a long time to fix, so it is a legitimate concern that the person might not be able to find housing to rent while cleaning up her credit report, since the report is essential to obtain a rental agreement.[125] Given these significant risks, a person might delay buying a new house.

The same concerns are true for employment. In the face of a heightened risk of identity theft, a person might delay looking for a new job because a polluted credit report can interfere with a person's employment opportunities. A person might not want to go through the time and effort of applying for a position if there is an increased chance that future employers will find her credit report marred by a thief's financial mischief. Seeking a new job could jeopardize one's current employment, so a reasonable person might not chance losing a current job in the face of an elevated risk that it will be

123. *See* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 125–27 (2011) (collecting a list of several cases in which organizations offered free credit monitoring to affected individuals after a data breach).

124. *E.g.*, Press Release, Off. of the Attorney Gen., St. of Conn., AG Jepsen to Anthem: End Unreasonable Delay in Providing Information to Affected Residents (Feb. 10, 2015), http://www.ct.gov/ag/cwp/view.asp?Q=560660&A=2341 [https://perma.cc/TA46-ZWJ5] (demanding that Anthem inform affected consumers within 24 hours that they are going to be provided two years of credit monitoring and identity-theft insurance to consumers impacted by data breach).

125. *"Big 3" Credit Bureaus Settle with 31 States Over Credit Reporting Mistakes*, CONSUMERS UNION (May 26, 2015), http://consumersunion.org/2015/05/big-3-credit-bureaus-settle-with-31-states-over-credit-reporting-mistakes/ [https://perma.cc/EEV6-7G7G] (explaining that one in five consumers have an error in their credit reports).

difficult to obtain a new one. Then too, a person might be chilled from seeking a job that requires a security clearance.[126]

Just as people might rationally delay an outdoor party when the forecast calls for a greater chance of rain, people might delay certain important life decisions when their risk of a sullied credit report increases.

Although the increased risk of harm as a result of a data breach might be hard to see, consider the following analogy. Imagine that a person owns two identical safes. She wants to sell them and lists them on eBay:

> SAFE FOR SALE
>
> Made of the thickest iron with the most unbreakable lock.

> SAFE FOR SALE
>
> Made of the thickest iron with the most unbreakable lock. However, the combination to the safe was improperly disclosed and others may know it. Unfortunately, the safe's combination cannot be reset.

Which safe would get the higher price?

Safe 2 is no longer as good as Safe 1. Its utility has been damaged by the improper disclosure of the combination to the safe, and thus the value of the safe has been significantly reduced.

Or suppose there is a new virus that does not cause adverse effects but that makes people more vulnerable to getting a painful disease later on. Many people will not develop the painful disease—only some will fall prey to it. Nonetheless, those with the virus are at greater risk to develop the painful disease. Has the person who has contracted the virus suffered harm?

In the case of the safe combination and the virus, people are made more vulnerable: they are placed in a weakened and more precarious position. Their risk level has increased. They are worse off than before the release of a safe's combination number or the exposure to a virus. In the immediate present, the increased risk exposure is undesirable, anxiety producing, and frustrating. In cases involving an increased risk of future harm, not all individuals will actually suffer that harm, but "each has suffered a loss in an actuarial sense because his chances of avoiding the harm have been reduced."[127]

---

126. Although Calo's scholarship has rejected the notion of risk as cognizable harm, the related out-of-pocket expenses and opportunity costs might fall under an expanded understanding of his view of objective harm.

127. David A. Fischer, *Tort Recovery for Loss of a Chance*, 36 WAKE FOREST L. REV. 605, 633 (2001). *See* Zehner v. Post Oak Oil Co., 640 P.2d 991, 994–95 (Okla. Civ. App. 1981) (allowing

People have a meaningful interest in avoiding risk.[128] They will go to the doctor to monitor their health. They will pay for insurance to insure against particular risks. Indeed, the insurance market is proof that protection against risk has a monetary value.

Although there are sophisticated ways to assess and understand risk, many courts have refused to recognize risk as a cognizable harm in data-breach cases. Risk is a central concept toward making more intelligent and practical decisions. As Justice Oliver Wendell Holmes famously observed, "the man of the future is the man of statistics and the master of economics."[129] And in many areas, law has recognized risk as a legally cognizable harm.

2. Legal Foundations for Recognizing Risk as a Cognizable Harm.— Data-breach harms may push on the edges of the law, but ample foundations and significant flexibility exist in the law to recognize them. The law has evolved to recognize risk. This trend is likely driven by the fact that modern thinking in science and business, among other domains, is deeply focused on risk. Because the conceptual underpinnings for recognizing data-breach harms are already present in the law, recognizing such harms does not require a radical shift in legal conceptions of harm. Risk so pervades modern thinking that law cannot resist embracing the concept if it is to remain relevant.

The law has grown in its recognition of future injury.[130] Over time, probabilistic injuries have been recognized in three conceptually related areas: increased risk of injury, loss of a chance, and fear of disease.[131] Tort law has developed to recognize the "fear of or the increased risk of developing a disease in the future" and "lost chances to avoid diseases or physical injury" as compensable injuries.[132] For these claims, the harm is the destruction of a future opportunity and the loss of hope.[133]

Courts have begun allowing people to sue for medical malpractice that results in the loss of an "opportunity to obtain a better degree of recovery."[134] Under risk-of-future-harm cases, damages include those "directly resulting

---

tort recovery as compensation for a lost chance to obtain a lease of land at a particularly profitable rate when the defendant committed the tort of slander of title).

128. Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 181 (1992).

129. OLIVER WENDELL HOLMES, *The Path of the Law*, *in* COLLECTED LEGAL PAPERS 167, 187 (1920).

130. Levit, *supra* note 128, at 154–55.

131. *Id.* at 154.

132. *Id.* at 154–55.

133. *Id.* at 158.

134. *E.g.*, Lord v. Lovett, 770 A.2d 1103, 1104–06 (N.H. 2001) (holding a medical malpractice plaintiff could recover for a lost chance at full recovery under the loss-of-opportunity doctrine); *see* Claire Finkelstein, *Is Risk a Harm?*, 151 U. PA. L. REV. 963, 985–86 (2003) (arguing tort law supports the notion of risk as a harm, and citing as a specific example lost-chance-of-recovery cases where medical malpractice plaintiffs are compensated for reduced chance of medical cure).

from the loss of a chance of achieving a more favorable outcome," as well as damages "for the mental distress from the realization that the patient's prospects of avoiding adverse past or future harm were tortiously destroyed or reduced," and damages "for the medical costs of monitoring the condition in order to detect and respond to a recurrence or complications."[135] For example, in *Petriello v. Kalman*,[136] a physician made an error that damaged the plaintiff's intestines.[137] The plaintiff was estimated to have between an 8% and 16% chance that she would suffer a future bowel obstruction.[138] The court concluded that the plaintiff should be compensated for the increased risk of developing the bowel obstruction "to the extent that the future harm is likely to occur."[139]

Similarly, environmental law is premised on the notion of risk as harm. "One of the major innovations of environmental law has been to substitute the concept of risk as a proxy for injury for the common law's insistence that injury be established by proof that an action in fact caused demonstrable harm."[140] Courts have found increased risk of disease sufficient for standing purposes and as the basis of regulation.[141]

To be sure, if remedies for increased risk of injury were applied broadly, many kinds of vulnerabilities would be prohibited. A driver who operates his car recklessly increases other drivers' potential to get into an accident. It would be difficult to imagine the law recognizing increased risk as harm due to reckless driving. In other cases, however, the law provides a remedy for increased risk of developing health complications due to medical malpractice. Why the different result? Once the reckless driver passes by traffic without getting into an accident, the risk has been eliminated. By contrast, the risk of developing future complications from medical malpractice may have no clear end in sight.

The risk of injury in a data-breach case is closer to the medical-malpractice scenario than that of the reckless driver. To the individuals whose personal data is leaked into the hands of thieves, the risk of harm is continuing. Hackers may not use the personal data in the near term to steal

---

135. Joseph H. King, Jr., *"Reduction of Likelihood" Reformulation and Other Retrofitting of the Loss-of-a-Chance Doctrine*, 28 U. MEM. L. REV. 491, 504–05 (1998).

136. 576 A.2d 474 (Conn. 1990).

137. *Id.* at 476.

138. *Id.* at 477.

139. *Id.* at 484.

140. ROBERT L. GLICKSMAN ET AL., ENVIRONMENTAL PROTECTION: LAW AND POLICY 738 (5th ed. 2007).

141. *E.g.*, Duke Power Co. v. Carolina Envtl. Study Grp., 438 U.S. 59, 74, 81 (1978) (holding the chance of "health and genetic" consequences resulting from exposure to radiation were sufficient to satisfy standing's injury-in-fact requirement); Ethyl Corp. v. EPA, 541 F.2d 1, 1, 12, 17 (D.C. Cir. 1976) (holding that the Clean Air Act empowers the EPA to regulate prophylactically against the risk of harm).

bank accounts and take out loans. Instead, they may wait until an illness befalls a family member and then use personal data to generate medical bills in a victim's name. They may use the personal data a year later but only use some individuals' personal information for fraud. Although not all of the personal data will be used for criminal ends, some will. In the meanwhile, the individuals worry that their information will be misused and expend time and resources to protect themselves from this possibility.

Long-term risk is not a harmless wrong, unlike the risky driver who does not hurt anyone. It is not negligence "in the air," which the law has long understood as unworthy of a legal response.[142] There is an injury; it is not a regrettable close call like the reckless driver who hits no one. When an entity inadequately secures personal data and thieves steal it, the entity's unreasonable actions impact a sizeable number of users, often in the millions,[143] and the excess risk of fraud is certain to take its toll on a number of those users. Victims spend time and money to minimize the impact of identity theft. They refrain from important life opportunities, such as buying a new home or looking for a new job. Over time, the risk of identity theft will materialize for a percentage of those users. Although the eventual victims cannot be immediately identified, the entity cannot deny the reality of the loss it has inflicted.

Law's recognition of risk of future harm was arguably anticipated by the Court in *Robins v. Spokeo* when the Court noted that intangible informational injuries, recognized at common law, can provide the basis for harm sufficient to support standing.[144] As shown by judicial doctrine related to lost chances, the common law has come to recognize increased risk of harm as an intangible injury worthy of redress.

There are practical implications of denying increased risk as a cognizable harm in data-breach cases. If increased risk is not understood as harm, then when the risk materializes, such as when the identity theft occurs, plaintiffs probably will be unable to sue at all. Statutes of limitations would likely bar any lawsuit.[145] Even if statutes of limitations are not a bar, delay in resolving the issue may lead to the loss of evidence.

---

142. *See* David Rosenberg, *The Causal Connection in Mass Exposure Cases: A "Public Law" Vision of the Tort System*, 97 HARV. L. REV. 849, 883 (1984) (explaining, in the mass exposure toxic tort setting, that torts creating long-term risk in a large enough group will inevitably manifest real injury, meaning the tortfeasor's wrongful conduct cannot be forgiven as "negligence in the air").

143. *See, e.g.*, Off. of the Att'y Gen., St. of Conn., *supra* note 124 (stating that the Anthem data breach "may have exposed sensitive personal information of as many as 80 million people, or perhaps more").

144. *See supra* notes 28–34 and accompanying text (discussing *Spokeo*).

145. Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 89 (2016).

In many other contexts, high-stakes decisions are based on risk, a fact that makes it difficult to understand why law should be an exception. Legal decisions are not necessarily more important than decisions in other domains; nor are people in the law inherently less capable of comprehending risk. Despite the law's caution and timidity with risk, it has been making significant steps toward embracing risk concepts. Risk-oriented harm has increasingly been recognized by the law, which has been catching up to more modern understandings of risk management. Changes in risk level have significant financial repercussions, and there are concrete and sophisticated approaches to evaluating, monetizing, and managing risk. Thus, the foundation is present for a more robust understanding of data-breach harm.

B. Anxiety as Harm

1. Understanding Anxiety.—Data-breach harms often result in victims experiencing anxiety about the increased risk of future harm. Anxiety is a form of emotional distress, which is an umbrella term to capture a wide array of negative and disruptive feelings such as sadness, embarrassment, and anxiety, among others.[146] With a data breach, anxiety is experienced as a result of knowing that personal information, often sensitive, can be observed and used to one's detriment.[147] Emotional distress is experienced in the present, but courts are reluctant to recognize it as a cognizable injury arising out of data-breach harms.

For breaches involving embarrassing or reputation-damaging information, plaintiffs clearly suffer emotional distress. Consider the breach of the Ashley Madison website, an online hub for individuals seeking sexual encounters outside of their relationships.[148] The hackers stole information related to users' sexual desires and personally identifying information and posted it online.[149] The knowledge that employers, family, and friends might discover one's intimate desires and fantasies produced significant anxiety.[150]

---

146. 2 DAN B. DOBBS, THE LAW OF TORTS § 302 (2001).

147. Calo, *Boundaries*, *supra* note 36, at 1148. As Calo argues and as we agree, there is real harm in the anxiety someone suffers due to the unwanted observation of personal information, such as the emotional distress suffered from knowing embarrassing information is lingering online or that a data breach could lead to identity theft. *See id.* at 1148–49 (describing the privacy harm that occurs where an individual worries observation could lead to the unanticipated use of personal information that will lead to "some adverse, real-world consequence").

148. Lisa Bonos, *Ashley Madison's Data Breach is a Warning for Us All, Cheaters or Not*, WASH. POST (July 20, 2015), https://www.washingtonpost.com/news/soloish/wp/2015/07/20/ashley-madisons-data-breach-is-a-warning-for-all-of-us-cheaters-or-not/ [https://perma.cc/6R6L-JTGM].

149. *Id.*

150. *See* Troy Hunt, *Here's What Ashley Madison Members Have Told Me*, TROY HUNT BLOG (Aug. 24, 2015), https://www.troyhunt.com/heres-what-ashley-madison-members-have/ [https://

Ashley Madison users who were active members of the military worried that they might face penalties because adultery is a punishable offense under the Army's Military Code of Conduct.[151] Following the breach, several affected individuals committed suicide.[152]

Many data breaches, however, do not involve embarrassing or discrediting information. The exposure of this information might not seem as intuitively harmful, but anxiety can be caused in many ways. Personal data involved in a breach is often a tool used for financial or identity fraud, and living under the specter of such fraud can make reasonable people worry that, at any moment, they might be impeded in making financial transactions, obtaining employment, or engaging in many other important activities.

A concern with recognizing emotional distress in data-breach cases is that psychic distress can be readily manufactured. Arguments against the recognition of anxiety focus on the fact that claims of anxiety are easy to make and difficult to dispute. Plaintiffs will quickly learn to make poignant statements about their anguish with details exaggerating their distress. Defendants may have difficulty disproving plaintiffs' accounts of their own subjective mental states.

Concerns over disingenuous claims of emotional distress as well as the difficulty in disproving such claims are certainly significant. But as we demonstrate in the next Part, the law has evolved to recognize emotional distress disconnected from physical or financial injury. In certain privacy cases, courts recognize pure emotional distress without hesitation,[153] most likely, we posit, because courts recognize that most people would feel emotional distress in these situations. In essence, an unstated objective test to emotional distress seems to exist in privacy tort cases.

Many other areas of law involve proving subjective mental states. Indeed, the vast majority of criminal law involves subjective mental states that must be proven with the highest standard of proof—beyond a reasonable doubt. Despite the challenges, the law quite often involves a quest to delve into the truth of what was going on in a person's mind.

---

perma.cc/3M24-9TJX] (detailing numerous anxious and worried reactions by Ashley Madison members after the breach).

151. Woodrow Hartzog & Danielle Citron, *Five Unexpected Lessons from the Ashley Madison Breach*, ARS TECHNICA (Dec. 29, 2016), http://arstechnica.com/tech-policy/2016/12/op-ed-five-unexpected-lessons-from-the-ashley-madison-breach/ [https://perma.cc/VK3W-UF34].

152. John Gibson, a pastor, took his own life six days after his name was released in the leak. His suicide note talked about his regret in using the site. *Id.* A San Antonio, Texas police captain committed suicide shortly after his email address was linked to an Ashley Madison account. *Id.*

153. *See, e.g.*, Doe v. Hofstetter, No. 11–cv–02209–DME–MJW, 2012 WL 2319052, at *8 (D. Colo. June 13, 2012) (awarding a plaintiff damages for alleged "severe emotional distress" in a default judgment without question); Daily Times Democrat v. Graham, 162 So.2d 474, 475–76, 478 (Ala. 1964) (affirming damages for a plaintiff who suffered embarrassment after defendant published a photo of plaintiff with her undergarments exposed).

A data breach can quite appropriately result in victims feeling anxiety. Leaks of personal data can cause embarrassment or result in fraudulent transactions. The most common preventative measure given to people is credit monitoring,[154] but this cannot inoculate data-breach victims against future injury. Credit monitoring merely informs people about anomalies in their credit reports after theft has occurred.[155] It does not prevent the misuse of data. By analogy, credit monitoring is akin to a blood-screening test for cancer. The test might indicate that a person has cancer, but the test is not a cure. Nor does routinely testing a person for cancer address the emotional suffering as a result of a person's increased risk of developing cancer.

Credit monitoring cannot totally alleviate a person's anxiety. Although credit monitoring will detect fraud appearing on a person's credit report, not all fraud will be documented in a victim's credit report. Fraudulent uses of leaked personal data that do not involve credit will often not be reported on a credit report. A credit report, for instance, will not alert a data-breach victim that a thief used her leaked personal information to empty her bank accounts.[156] It will not notify a data-breach victim that a fraudster has used her leaked login credentials to access private files on her computer or used her computer to send out spam.[157]

Data breaches can create a cascade of compromised accounts, especially if they involve personal data about password-recovery questions. Because there is no ready expiration date on the misuse of compromised personal data, criminals can at any point use that information to defraud victims. Anxiety about this increased risk, which often cannot be fully reduced, is a legitimate, real, and discomfiting experience.

Anxiety over a data breach is often dismissed as the irrational response of abnormally anxious people. But it is rational for people to feel anxiety about the fact that their personal data is in the hands of criminals who can cause their financial ruin. A blizzard of laws protects data security, the reality of which demonstrates that data breaches are not a trivial matter to

154. *See, e.g.*, Galaria v. Nationwide Mut. Ins., 663 F. App'x 384, 386 (6th Cir. 2016) (noting that in response to a breach of its computer networks, the defendant offered free credit monitoring to its customers); Press Release, Equifax, Inc., Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832 [https://perma.cc/U2CE-KQJR] (highlighting that in response to a data breach, Equifax offered free credit monitoring to all of its customers).

155. U.S. GOV'T ACCOUNTABILITY OFF., GAO-17-254, IDENTITY THEFT SERVICES: SERVICES OFFER SOME BENEFITS BUT ARE LIMITED IN PREVENTING FRAUD 10 (2017).

156. *Identity Theft Protection Services*, FED. TRADE COMM'N: CONSUMER INFO. (Mar. 2016), https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services#monitoring [https://perma.cc/X779-MMT3].

157. *See id.* ("Credit monitoring only warns you about activity that shows up on your credit report.").

legislatures. The media often report on data breaches,[158] and it is rational to assume that the media is paying attention because data breaches cause some kind of harm. Otherwise, why report on something that should generate no worries or concerns?

People are often advised to take steps to protect their personal data, such as Social Security numbers.[159] They are told to shred documents with sensitive personal data and to avoid carrying such data around in their wallets.[160] Rational people would assume that these measures are meant to prevent something harmful from happening. Otherwise, why bother if there is nothing to worry about? It seems reasonable for a person to respond to a data breach with anxiety in light of all the attention and concern given to data breaches. So much focus is not typically given to something that is benign. Moreover, many organizations stress that keeping personal data secure is very important to them.[161] If failing to do so should not cause people any anxiety, then why bother promising to keep the data secure? It would be absurd for organizations to worry about data breaches if victims have nothing to be concerned about.

2. Legal Foundations for Recognizing Anxiety as Harm.—Ample foundations exist in the law to recognize anxiety as a cognizable harm. There was a time when pure emotional distress was discounted because it seemed

158. *See, e.g.*, Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news [https://perma.cc/D9E6-BXGW] (discussing the 2017 Equifax cyberattack that resulted in a breach of sensitive consumer information); Rishi Iyengar, *Hackers Release Data from Cheating Website Ashley Madison Online*, TIME (Aug. 18, 2015), http://time.com/4002647/ashley-madison-hackers-data-released-impact-team/?iid=sr-link1 [https://perma.cc/37Y3-WHAP] (detailing the 2015 data breach of Ashley Madison that revealed members' personal and financial data); Maggie McGrath, *Target Data Breach Spilled Info On As Many As 70 Million Customers*, FORBES (Jan. 10, 2014), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#528bf61ee795 [https://perma.cc/XQ6V-GUSK] (reporting on the breach of customer information at Target in late 2013).

159. *See How to Keep Your Personal Information Secure*, FED. TRADE COMM'N: CONSUMER INFO. (July 2012), https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure [https://perma.cc/H7QF-JZN3] (detailing suggestions for protecting personal information to avoid identity theft).

160. *Id.*

161. *See, e.g.*, AMAZON WEB SERVS., AMAZON WEB SERVICES: OVERVIEW OF SECURITY PROCESSES 1 (2017), https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf [https://perma.cc/8KR8-QQFT] ("Helping to protect the confidentiality, integrity, and availability of our customers' systems and data is of the utmost importance . . . ."); *This Is How We Protect Your Privacy*, APPLE INC., https://www.apple.com/privacy/approach-to-privacy/ [https://perma.cc/ZQC8-4B8H] ("We're committed to keeping your personal information safe.").

too ethereal, too difficult to measure, too easy to fake.[162] That view of emotional distress faded in the mid-twentieth century.[163] It has been replaced by a much greater and growing acceptance of emotional distress as a cognizable harm.

The law has grown to recognize so-called "ethereal" harms.[164] In some instances, the recognition of emotional distress traces its roots back before the modern era. As Ryan Calo has argued, the "tort of assault—where the harm is the emotion of fear—dates back six and a half centuries."[165] It redressed emotional distress without any showing of physical injury.[166] Relational torts like the alienation of affection, of a similar vintage, permitted compensation for emotional distress.[167]

Privacy law's roots supported the recognition of emotional distress as a compensable injury in the early twentieth century. In *The Right to Privacy*,[168] Samuel Warren and Louis Brandeis spent considerable energy discussing the evolving nature of harm, from tangible to intangible injuries. "[I]n very early times," they contended, "the law gave a remedy only for physical interference with life and property."[169] 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."[170] Property developed to include "every form of

162. *See* Levit, *supra* note 128, at 172 (arguing that courts effectively exercise "a presumption that claims of mental disturbance are frivolous"); Leslie Benton Sandor & Carol Berry, *Recovery for Negligent Infliction of Emotional Distress Attendant to Economic Loss: A Reassessment*, 37 ARIZ. L. REV. 1247, 1253 (1995) (exploring fears about triviality, fraudulent claims, and unmanageability that accompany resistance to emotional distress torts). Emotional distress was also dismissed as the province of the neurotic, weak-minded, and deviant. *See* Rodrigues v. State, 472 P.2d 509, 520 (Haw. 1970) (addressing the argument that "mental distress of a trivial and transient nature are part and parcel of everyday life" and that the law should not "curry to neurotic patterns in the population"); Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 393 (2009) (describing the persistent historical trivialization of women's emotional distress and dismissal of attendant tort claims). Amanda Pustilnik insightfully explores the law's tendency to refuse damages for pain and suffering because plaintiffs were viewed as mentally ill, hysterical, or fraudsters. A.C. Pustilnik, *Imaging Brains, Changing Minds: How Pain Neuroimaging Can Inform the Law*, 66 ALA. L. REV. 1099, 1107–12 (2015).

163. *See* Robert L. Rabin, *Emotional Distress in Tort Law: Themes of Constraint*, 44 WAKE FOREST L. REV. 1197, 1197 (2009) (explaining that emotional distress "gained respectability" as a stand-alone tort claim with the adoption of intentional and negligent infliction of emotional distress into the Restatement (Second) of Torts in 1948 and 1960 respectively).

164. Levit, *supra* note 128, at 158.

165. Calo, *Exceptionalism*, *supra* note 35, at 363.

166. Rabin, *supra* note 163, at 1197.

167. *Id.*

168. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

169. *Id.*

170. *Id.* at 194.

possession—intangible, as well as tangible."[171] Defamation law protected reputations without requiring proof of financial or physical suffering. The harm involved a person's good name rather than a tangible loss.[172]

In tracing law's development surrounding the nature of harm, Warren and Brandeis were paving the way for the legal recognition of remedies for privacy invasions, which primarily involve an "injury to the feelings."[173] Warren and Brandeis identified the legally protected interest set back by privacy invasions as a person's ability to develop her "inviolate" personality.[174] Privacy invasions inflict harm by interfering with a person's ability to decide the extent to which her personal information would be revealed, shared, and disclosed to others. Warren and Brandeis noted that privacy invasions interfere with a person's "estimate of himself," inflicting "mental pain and distress, far greater than could be inflicted by mere bodily injury."[175]

In the century following the publication of the Warren and Brandeis article, the law grew to recognize privacy torts because emotional tranquility was an interest deserving protection.[176] Courts recognized that emotional distress could be "as severe and debilitating as physical harm."[177] Privacy tort claims have succeeded in garnering compensation for emotional distress.[178] Plaintiffs have prevailed in cases involving the dissemination of nude photos,[179] before-and-after photos of plastic-surgery patients,[180] and autopsy

171. *Id.* at 193.

172. *Id.* at 197. Defamation liability includes redress for emotional distress caused by the defamatory publication. RESTATEMENT (SECOND) OF TORTS § 623 (AM. LAW INST. 1977).

173. Warren & Brandeis, *supra* note 168, at 197.

174. *Id.* at 205, 211.

175. *Id.* at 196–97.

176. *See* Calvert Magruder, *Mental and Emotional Disturbance in the Law of Torts*, 49 HARV. L. REV. 1033, 1035–36 (1936) (explaining that most jurisdictions had begun to allow recovery for outrage and emotional distress, abandoning the common law view that peace of mind is not worthy of legal protection).

177. *E.g.*, Molien v. Kaiser Found. Hosps., 616 P.2d 813, 814 (Cal. 1980); Schultz v. Barberton Glass Co., 447 N.E.2d 109, 113 (Ohio 1983) (citing *Molien*).

178. *See* Citron, *Mainstreaming*, *supra* note 36, at 1811–14 (2010) (exploring privacy tort cases awarding damages for emotional distress, mental anguish, worry, and embarrassment).

179. Daily Times Democrat v. Graham, 162 So.2d 474, 475–76, 478 (Ala. 1964) (awarding damages for embarrassment and humiliation after a newspaper published a picture of the plaintiff whose undergarments were exposed after wind blew up her skirt); Doe v. Hofstetter, No. 11-cv-02209-DME-MJW, 2012 WL 2319052, at *7 (D. Colo. June 13, 2012) (awarding, in a default judgment, damages for intentional infliction of emotional distress and public disclosure of private fact where the complaint alleged the defendant had posted intimate photographs of the plaintiff online, emailed them to plaintiff's husband, and created fake Twitter accounts displaying them).

180. Vassiliades v. Garfinckel's, Brooks Bros., Miller & Rhoades, Inc., 492 A.2d 580, 585–86, 594–95 (D.C. 1985).

or death-scene photos of loved ones.[181] Courts do not question the harm in those cases, even though it involves intangible injury.[182] Indeed, with corpse photos, courts recognize that the photos implicate the privacy rights not of the subject of the photos (the dead person) but of the deceased person's family members.[183]

The privacy torts readily allow for emotional distress damages alone. As David Elder aptly notes in his treatise *Privacy Torts*, decisions on the public-disclosure-of-private-fact tort "collectively reject any suggestion that special damages or physical injuries are a threshold pre-condition to recovery."[184] Elder explains that courts have permitted harms such as "injury to feelings or sensibilities; feelings of violation and mortification; . . . fear for physical security; . . . past and future humiliation; [and] embarrassment," among other things.[185] According to the Restatement of Torts, plaintiffs can recover for purely emotional distress harm.[186] As one court put it, plaintiffs are "entitled to recover substantial damages, although the only damages suffered . . . resulted from mental anguish."[187]

Under the tort of intrusion upon seclusion, mental distress is "recoverable without the necessity of showing actual physical injury . . . because the injury is essentially . . . subjective, not actual harm done to the plaintiff's body."[188] As a court noted: "The difficulty of measuring damages for invasion of privacy is no reason for denying relief."[189] Elder observes that

> Since the gravamen of the tort is "injury to the feelings of the plaintiff, and the mental anguish and distress caused thereby," the plaintiff is generally entitled to collect substantial damages, "damages of real

181. Catsouras v. Dep't of the Cal. Highway Patrol, 104 Cal. Rptr. 3d 352, 359, 385 (Cal. Ct. App. 2010) (concerning automobile death scene photos); Douglas v. Stokes, 149 S.W. 849, 849–50 (Ky. 1912) (concerning autopsy photos of conjoined twins). A family's privacy interest in death images of deceased persons was also recognized by the U.S. Supreme Court as a valid basis to assert a privacy exemption to the Freedom of Information Act (FOIA). *See* Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 168, 174–75 (2004) ("Family members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own.").

182. *See* Citron, *Mainstreaming*, *supra* note 36, at 1811–14 (noting courts' recognition of mental and privacy harms across a variety of privacy torts).

183. *See Catsouras*, 104 Cal. Rptr. 3d at 394 (concluding that the plaintiffs had a privacy interest in preventing the dissemination of gruesome photographs of their deceased loved one); *Stokes*, 149 S.W. at 849–50 (affirming that the defendant–photographer violated the plaintiff's privacy when he wrongfully used photographs of the plaintiff's dead children for his own benefit).

184. ELDER, *supra* note 47, at § 3:8.

185. *Id.*

186. RESTATEMENT (SECOND) OF TORTS § 652H cmt. b (AM. LAW. INST. 1977).

187. Brents v. Morgan, 299 S.W. 967, 971 (Ky. 1927).

188. Gonzales v. Sw. Bell Tel. Co., 555 S.W.2d 219, 221–22 (Tex. Civ. App.—Corpus Christi 1977) (quotation marks omitted) (quoting Billings v. Atkinson, 489 S.W.2d 858, 861 (Tex. 1973)).

189. Socialist Workers Party v. Attorney Gen., 642 F. Supp. 1357, 1422 (S.D.N.Y. 1986).

> worth and importance," for emotional distress without any proof of special damages or physical or otherwise debilitating psychic injury.[190]

Courts have also recognized emotional harm for the breach-of-confidentiality tort. The law recognizes that disclosures of information made in confidential relationships involve "harms of broken trust, betrayal, and disrupted expectations of secrecy."[191] Suppose a doctor improperly breaches patient confidentiality and reveals the patient's medical data to another person. The data is not embarrassing; the patient is in good health, and there is nothing embarrassing revealed and no reputational damage done. Is the patient harmed? Courts readily recognize harm under these circumstances. The harm involves the betrayal of trust in socially desirable professional relationships. As Elder notes, "The permissible damages are broad and parallel those available under the intrusion and other privacy torts."[192] Additionally, in other contexts, courts accept emotional distress damages based solely upon the plaintiff's testimony, such as in employment-discrimination cases.[193]

In case after case involving the privacy torts and breach-of-confidentiality tort, courts have recognized harm based on pure emotional distress or psychological impairment. Fear, anxiety, embarrassment, and loss of trust are all recognized as harms.[194] Humiliation, nervousness, worry, and loss of sleep are understood as compensable harms.[195]

The inconsistency between these different contexts is quite stark. Bodies of tort jurisprudence are entirely ignored in cases involving data-breach harms. Courts do not distinguish these cases; they simply do not mention them, as if those cases did not exist as precedent. Hardly any attempt is made to reconcile them. In contrast to cases involving data breaches, cases involving the privacy torts and breach-of-confidentiality tort lack the judicial hand-wringing and angst over the recognition of emotional harm.

The common law has also recognized claims for intentional infliction of emotional distress as well as for negligent infliction of emotional distress.[196] Claims for negligent infliction of emotional distress initially were limited to

---

190. ELDER, *supra* note 47, § 2:10.

191. Levit, *supra* note 128, at 147–48.

192. ELDER, *supra* note 47, at § 5:2.

193. Lewis R. Hagood, *Claims of Mental and Emotional Damages in Employment Discrimination Cases*, 29 U. MEM. L. REV. 577, 586 (1999) ("[A] majority of the federal courts that have held a plaintiff's own testimony as sufficient to sustain an award of damages for emotional distress usually subject such claims to heightened scrutiny.").

194. *See* Citron, *Mainstreaming*, *supra* note 36, at 1811–14 (offering examples of mental injuries resulting from privacy intrusions).

195. *Id.* at 1811.

196. Keating, *supra* note 54, at 277 & n.18.

cases involving physical injury, but that rule eased over time.[197] In the past fifty years, courts have deemphasized the "directness of the physical injury" and emphasized the "reality of the emotional distress suffered by the plaintiff."[198] Courts have recognized negligent-infliction-of-emotional-distress claims where the emotional distress occurs in the context of relationships that impose independent, preexisting duties of care.[199]

Relevant to data-breach cases, in a series of cases, courts have permitted emotional distress damages for fear of contracting diseases. Courts have held that plaintiffs can recover for fear of contracting AIDS, even if they do not yet have AIDS and even if they are not HIV positive.[200] For example, in *Johnson v. West Virginia University Hospitals, Inc.*,[201] the court held that a police officer could sue for emotional distress caused by the fear of contracting AIDS after being bitten by an AIDS patient.[202] Although a majority of courts require plaintiffs to prove actual exposure to HIV,[203] a number of courts do not require exposure to HIV to warrant recovery for emotional distress.[204] Courts have also permitted emotional distress damages based on fear of contracting cancer. In one case, a court held that the

197. *See* Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CALIF. L. REV. 722, 814–15 (1985) (describing the tests of varying stringency courts have applied to emotional distress claims).

198. Levit, *supra* note 28, at 144.

199. Keating, *supra* note 54, at 278.

200. Vance A. Fink, Jr., *Emotional Distress Damages for Fear of Contracting AIDS: Should Plaintiffs Have to Show Exposure to HIV?*, 99 DICK. L. REV. 779, 794 (1995); James C. Maroulis, Note, *Can HIV-Negative Plaintiffs Recover Emotional Distress Damages for Their Fear of AIDS?*, 62 FORDHAM L. REV. 225, 237–39, 247 (1993).

201. 413 S.E.2d 889 (W. Va. 1991).

202. *Id.* at 891, 894.

203. Majca v. Beekil, 701 N.E.2d 1084, 1089 (Ill. 1998) ("[A] majority of the courts that have considered claims for fear of contracting AIDS have required a showing of actual exposure to HIV."). Some of the cases cited in *Majca* include: *Brzoska v. Olson*, 668 A.2d 1355 (Del. 1995); *K.A.C. v. Benson*, 527 N.W.2d 553 (Minn. 1995); *Bain v. Wells*, 936 S.W.2d 618 (Tenn. 1997); *Johnson v. West Virginia University Hospitals, Inc.*, 413 S.E.2d 889 (1991); and *Neal v. Neal*, 873 P.2d 871 (1994). *Majca*, 701 N.E.2d at 1089.

204. *See* Hartwig v. Or. Trail Eye Clinic, 580 N.W.2d 86, 94 (Neb. 1998) (allowing plaintiffs to recover for mental anguish even when it cannot be determined whether the tissue, blood, or body fluid may be HIV positive); Williamson v. Waldman, 696 A.2d 14, 21–22 (N.J. 1997) (rejecting the actual-exposure requirement and allowing emotional distress damage for plaintiffs who could show genuine, reasonable emotional distress); Madrid v. Lincoln Cty. Med. Ctr., 923 P.2d 1154, 1160–61, 1163 (N.M. 1996) (holding an emotional distress plaintiff must only prove contact with a channel medically capable of transmitting HIV, regardless of whether HIV was present at the time of contact); Faya v. Almaraz, 620 A.2d 327, 337 (Md. 1993) (holding plaintiffs can recover for fear of contracting AIDS when the fear is during the reasonable window of anxiety); *see also* Marchica v. Long Island R.R. Co., 31 F.3d 1197, 1206–07 (2d Cir. 1994) (holding that despite medical uncertainty as to how the HIV virus could be transmitted through a needle, plaintiff's contact with an HIV-positive needle was sufficient to support a fear-of-developing-disease claim).

plaintiff's fear of getting cancer after being exposed to asbestos was reasonable and actionable.[205]

The harm from an increased risk of identity theft is akin to the risk of contracting a chronic disease. The risk of a data breach is ongoing. Data-breach notification letters explicitly inform people that there is a risk of identity theft. Credit-monitoring services are offered for one or two years,[206] signaling to plaintiffs an increased risk of theft for that time period. When a person has a reasonable belief that her credit identity is in jeopardy, she is rightly afraid that her creditworthiness is out of her hands. The exposure to the risk of identity theft can be anxiety-inducing because identity theft can have catastrophic effects on an individual's life and because it is difficult to resolve. The passage of time may not dissipate that fear because identity theft can happen at any time. A person's financial and employment opportunities can be destroyed by identity theft, and time and money are essential to addressing it. In all of these ways, identity theft is the digital equivalent to contracting a chronic disease.

The clear direction and thrust of the law is towards a greater recognition of emotional distress. In various contexts, the law has increasingly recognized pure emotional distress as cognizable harm. Negligent infliction of emotional distress has moved beyond the narrow confines of physical harm to extend to certain relationships requiring a duty of care.[207] These bodies of law have laid the foundation to extend emotional distress damages to cases involving inadequate security.[208]

Thus, there is a robust basis in the law to recognize the intangible nature of data-breach harms. In tort cases, courts have recognized emotional distress

---

205. Devlin v. Johns–Manville Corp., 495 A.2d 495, 498–99 (N.J. Super. Ct. Law Div. 1985).

206. *See* Robert Harrow, *What For-Pay Credit Monitoring Services Actually Offer*, FORBES (Sept. 25, 2017), https://www.forbes.com/sites/robertharrow/2017/09/25/what-for-pay-credit-monitoring-services-actually-offer/#62a9303579bc [https://perma.cc/Z5Y3-ELPD] (explaining that Equifax has offered a one-year credit-monitoring service); *How FDIC Is Helping*, FDIC (Nov. 1, 2016), https://www.fdic.gov/creditmonitoring/howfdicishelping.html [https://perma.cc/W4GK-UQL9] (offering a two-year credit-monitoring service for individuals affected by FDIC security incidents).

207. The Reporters' Memorandum to tentative drafts of the Restatement (Third) of Torts: Liability for Physical and Emotional Harm explains that there is a "recurring (and new) theme"—the use of "arbitrary lines to limit recovery for emotional disturbance." *Reporters' Memorandum* to RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM xxi (AM. LAW INST., Tentative Draft No. 5, 2007). The Reporters' Memorandum recognizes that the restrictions are arbitrary but that "given the ubiquity of emotional disturbance, lines must be drawn." *Id.*

208. For further discussion on how the foundation of tort law can be adopted to modern cyber-security issues, see generally Citron, *Mainstreaming*, *supra* note 35 (detailing the foundation created from existing privacy tort law and suggesting how to adapt existing tort law to fit modern cyber issues); Citron, *Reservoirs*, *supra* note 35 (analyzing the use of tort law to combat the current cyber crisis and offering suggestions for how the law should adapt to meet the changing challenges of the Information Age).

alone as sufficient for harm. These cases typically involve privacy torts and breach of confidentiality rather than negligence. Nonetheless, the precedent is there to recognize emotional distress as cognizable harm in data-breach cases. In contract cases, courts recognize the value of preferences without economic value.

III. An Approach for Assessing Risk and Anxiety

Many courts reject risk and anxiety as cognizable harms based upon concerns about the difficulty of assessing and quantifying a dollar value for risk and anxiety. Courts worry that plaintiffs can simply assert a desire for redress for increased risk and anxiety and that there is no way to evaluate their claims with rigor or concreteness. Courts express concern that preventative measures to protect against future injury are merely "manufactured" to generate cost. The overarching concern is that risk and anxiety are speculative, subjective and, worse, susceptible to manipulation by attorneys who desire to manufacture injuries out of a data breach.

In this Part, we contend that risk and anxiety can be assessed in a sufficiently concrete way. Although risk might be difficult to measure with precision, factors exist that can be measured and quantified. Courts should determine whether a reasonable person would take preventative measures and, if so, assess the harm based on the reasonable cost of such measures. Whether, in fact, plaintiffs actually took such measures should not be the focus, as the test we propose is objective. In essence, risk can be assessed based on what it would cost to insure against such risk. A similar approach is suggested for anxiety. Courts should employ an objective standard, assessing whether a reasonable person would feel anxiety over any unmitigated risk of future injury stemming from a data breach.

A. Assessing Risk

1. Likelihood and Magnitude of the Future Injury.—Courts should examine how the use or disclosure of the personal data would affect the financial security, reputation, or emotional state of a reasonable person. If stolen data is posted on sites used by identity thieves, then a substantial risk exists that the data will be used for fraudulent ends.[209] On the other hand, if a thief steals a car with a password-protected laptop and the data is encrypted, then there is little to suggest a substantial risk of identity theft.

From a risk perspective, the likelihood and magnitude of future injuries fall on a sliding scale. A significant risk can exist with a low likelihood of a

209. *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014) (noting that the stolen personal information had surfaced on the Internet and describing the risk of misuse as impending and very real).

high-magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood is a risk worthy of concern.

In many cases, it can be challenging to assess the likelihood and magnitude of future injury with any degree of scientific precision. This is because the potential uses of the data are vast. Nonetheless, there are factors that suggest the likelihood and magnitude of future injury. Courts can assess how different types of data have been misused in the aftermath of similar data breaches. Courts can look at the means and methods used to exploit different types of data involved in data breaches. Courts should examine the extent that breached data can be aggregated with other available data and the harms that result from the use of the aggregated data.

2. Data Sensitivity and Data Exposure.—Certain types of data are readily categorized as sensitive because their release poses a substantial risk of being used to perpetrate fraud and identity theft. Some personal data effectively amount to keys to a bank account, such as account information coupled with passwords, Social Security numbers coupled with driver's license numbers, and medical-insurance information coupled with dates of birth.

Information can be sensitive if it reveals embarrassing or reputation-damaging matters that a reasonable person would want to conceal from others. The Ashley Madison hack resulted in the posting of highly sensitive information about married people's desire to have sex with strangers and information about their sexual preferences.[210] Beyond the embarrassment and humiliation, that data raises the substantial risk of bribery and extortion.

These situations are easily understood as raising a substantial risk of fraud, embarrassment, or reputational damage. But that is not to suggest that the harm from data breaches involving more innocuous-seeming personal data is trivial. Personal data does not exist in a vacuum. It can be readily combined with other data to reveal sensitive information and thus cause harm to individuals. For instance, it might seem trivial if information about people's mothers' maiden names is compromised, but this data is often used for password-recovery questions and could compromise the security of personal accounts. The same is true for data about people's favorite books, places of birth, and other facts that might not, in isolation, seem to be sensitive.

Compromised data does not exist in a void. The world is teeming with data, and compromised data can be readily combined with data to cause harm to individuals. It is nearly impossible to figure out in advance all the possible

210. Sakinah Jones, Note, *Having an Affair May Shorten Your Life: The Ashley Madison Suicides*, 33 GA. ST. U. L. REV. 455, 455, 457 (2017).

combinations and permutations. But one thing is clear: As more data about a person is compromised, it will become increasingly more possible to make data combinations that could be used to injure individuals.

The sensitivity of data—and its potential to cause harm—can be the result of the data itself like Social Security numbers combined with birth dates. But it also can be the result of the aggregation of seemingly innocuous data with other data. Sensitivity and harmfulness stem from the potential uses of the data, and data is often not used in isolation. Because of these facts, courts should be careful to avoid rushing to a conclusion that compromised data will not cause harm just because the data might appear to be innocuous.

3. Mitigating Actions.—Another consideration is whether the potential harm is reasonably likely to be mitigated by other actions. Consider the leak of credit card numbers. Although credit card companies are not required to reimburse customers for all fraudulent charges,[211] many major credit card companies have a zero-fraud liability policy.[212] Thus, where reasonable costs are likely to be reimbursed, this consideration should be kept in mind when assessing the likelihood of the harm.

4. The Reasonableness of Preventative Measures.—Preventative measures to reduce harm can serve as guideposts to understanding risk in more concrete terms and to figuring out the current costs of future harm. What preventative measures are available to deal with a potential future harm? What are the costs and effectiveness of such measures? In the absence of efficient preventative measures, what would it cost to insure against the risk of future harm if such insurance were available?

The ultimate barometer for this analysis is reasonableness. Courts should look at the degree of the risk. If there is significant uncertainty, courts should assess the reasonableness of trying to manage the uncertainty. A component of reasonableness would be evaluating the cost of preventative measures in relation to their potential benefit. Costly measures for a small chance of a modest harm would be unreasonable. Inexpensive measures for a small chance of a significant harm, however, would be reasonable—these considerations are the basis of contemporary insurance markets.

The objection that plaintiffs can manufacture harms by incurring the costs of preventative measures would have no bearing on our objective test. It would not matter whether plaintiffs choose unreasonably expensive preventative measures or whether they pursue no preventative measures at all. An objective approach avoids the problem of the overly sensitive

211. *See* 15 U.S.C. § 1643(a) (2012) (limiting but not disallowing cardholder liability for unauthorized credit card use); Regulation Z, 12 C.F.R. § 226.12(b) (2017) (same).

212. Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015).

plaintiffs or the overly cavalier ones. Courts do not need to take plaintiffs' word for these things.

In *Clapper*, the U.S. Supreme Court failed to understand risk. The Court expressed deep concern about people spending money on protective measures to manufacture standing.[213] But there are ways to distinguish genuine measures from manufactured ones. The key issue that the Court should have analyzed in *Clapper* is whether the decision to take any given measure was a reasonable response to the risk of government surveillance. Instead of certainties, we need to shift the focus to risk because contemporary understandings of the world are based on risk. This is how most of the business and scientific world operates—by seeing things through the lens of risk. Moreover, a requirement of reasonableness will limit the ability of any plaintiff to manufacture standing. Courts can analyze whether a person would be reasonable in assessing the risk of surveillance (or fraud) and in undertaking preventative measures to address that risk.

B. Assessing Anxiety

As the law has recognized in other contexts, emotional distress should count as a sufficient basis to establish harm. A data breach might not exact immediate financial costs to people, but the leak puts people's good credit history at risk of being blemished by fraudulent transactions in the future. That one's credit is in jeopardy of becoming polluted can be the source of considerable anxiety, especially for people who anticipate engaging in pursuits involving their credit, such as buying a new home or looking for a new job. A data breach can raise a person's risk of reputational damage, as seen in the Ashley Madison hack, and in turn result in significant anxiety.[214]

But not every instance of emotional distress should be cognizable. Courts should assess whether a plaintiff's emotional distress is reasonable under the plaintiff's particular circumstances. This would help exclude disingenuous claims and those made by hypersensitive people. Reasonableness inquiries have weeded out frivolous claims of emotional harm elsewhere in the law and can do so in data-breach cases.

Elements of certain claims can be viewed as protecting against frivolous attempts at recovery for emotional distress. Consider claims for intrusion on seclusion and public disclosure of private-fact torts: they provide redress only for privacy invasions that would be "highly offensive to the reasonable

213. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 407–08 (2013).

214. *See* Troy Hunt, *Here's What Ashley Madison Members Have Told Me*, TROY HUNT BLOG (Aug. 24, 2015), https://www.troyhunt.com/heres-what-ashley-madison-members-have/ [https://perma.cc/3M24-9TJX] (detailing numerous anxious and worried reactions by Ashley Madison members after the breach).

person."[215] Intentional infliction of emotional distress claims can succeed only if plaintiffs can show that their anxiety was caused by "extreme and outrageous" conduct.[216] How might courts approximate such protections in negligence claims? Here too we can look to current applications of negligence law. Courts can assess whether the emotional distress is serious and genuine, as is done in cases involving workers with asbestosis who fear their increased likelihood of developing cancer.[217]

C. Examples

The nature of a data breach provides significant insight into the way courts should understand and estimate the nature of the risk and accompanying anxiety. Consider the following spectrum of scenarios:

1. Attempted Fraud Against the Plaintiff.—Let's consider a data breach where hackers attempt to use an individual's information for fraudulent purposes. As discussed in Part I, courts have found that if hackers obtain a plaintiff's personal data and use it for fraudulent ends, there is little debate about the existence of harm. Situations involving attempted fraud should be viewed in similar terms. They generally present sufficiently concrete evidence of a significant risk of injury. There is a very high risk of future injury in such cases, and courts should recognize that risk as cognizable harm.

Suppose a fraudster obtains a plaintiff's personal data and sells the data online to other criminals. Although no one has attempted to use the information yet, a substantial risk exists that this will happen. Courts should find harm under these circumstances. The only thing to cut against the risk of injury is if the data by itself or in combination with other data poses little risk of potential criminal use. That would be true of data stripped of indicia that could be used to reasonably connect it to specific individuals.[218]

To return to a recent decision, in *Bradix v. Advance Stores Co., Inc.*,[219] the court dismissed claims for lack of injury where the plaintiff alleged that hackers obtained the defendant's employees' names, Social Security numbers, gross wages, and states where employees pay income taxes and used that information in unauthorized attempts to secure vehicle financing

---

215. Citron, *Mainstreaming*, *supra* note 36, at 1827.

216. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 121 (2014).

217. *E.g.*, Norfolk & W. Ry. Co. v. Ayers, 538 U.S. 135, 157–58 (2003) (allowing claims for damages for emotional distress resulting from the fear of developing cancer so long as the plaintiff proves the genuine and serious nature of the fear).

218. *But see* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1845 (2011) (describing the difficulty of stripping personally identifying information of the indicia that connect it to specific individuals).

219. No. 16-4902, 2016 WL 3617717 (E.D. La. July 6, 2016).

appearing on the plaintiff's credit report. The court based its dismissal on the fact that there was no proof that the attempts at fraud had actually damaged the plaintiff's credit score.[220] That hackers had personal data and attempted to use it makes clear that there is a significant risk of future injury. Hackers—whose identities are unknown and who remain at large—can use and will likely use the information for criminal ends sometime in the future. The past efforts of hackers make clear their intent to use personal data for fraud. The sensitive nature of the data increases the likelihood that hackers will be successful in future efforts to steal individuals' identities for fraudulent purposes. Crucially, there is little that plaintiffs can do to mitigate the harm since Social Security numbers and names cannot be changed to avoid future fraud.

2. Actual or Attempted Fraud Against Others.—Suppose a hacker obtains personal data of hundreds of individuals, including the plaintiff. The fraudster defrauds, or attempts to defraud, some of these individuals, but not the plaintiff. That hackers have victimized or have attempted to defraud individuals similarly situated to the plaintiff should be sufficient to establish a substantial risk of future injury.

3. Fraudster Obtains Personal Data But Use Remains Unknown.—In a number of circumstances, fraudsters obtain plaintiffs' personal data, but nothing is known about their misuse. In those circumstances, the precise motives of criminal hackers may be unknown. It is fair, however, to suggest that there is a substantial likelihood that hackers hope to use the data for criminal ends. Courts should not require proof that hackers had criminal motives. As a practical matter, the hackers' identities are unknown and thus such proof is elusive. Crucially, there is no need to require it. Hackers' criminal motives can be presumed. As the Seventh Circuit asked in *Remijas*, why else would hackers steal personal data if not for criminal purposes?[221] If a burglar breaks into a house and takes the jewelry box, it is logical to assume that the burglar is interested in the jewelry.

Again, much like the analysis of attempted fraudulent uses of personal data, courts should consider the types of personal data stolen and whether that data alone or combined with other data is likely to be used for fraud. Courts also should take into consideration if there are avenues for plaintiffs to prevent or curtail potential fraudulent uses of the data.

4. Stolen Electronic Device with Personal Data.—Suppose a thief steals a portable electronic device containing a plaintiff's personal data. Nothing is

220. *Id.* at *1, *4.

221. *See supra* notes 24–26 and accompanying text.

known about the use of the data. The device might have been stolen for the device or the data. Thus, the risk of misuse of data is unclear. To assess whether the device was likely stolen for the data stored inside or the hardware, courts can ask whether such devices have a significant market value independent of the data, whether the thief might have known of the nature of the data on the device, the nature of the data on the device and its sensitivity, and other things.

This case could go either way. If the data by itself or in combination with other data is not readily usable for fraud, then this cuts strongly against harm.

If the data is encrypted—and if the encryption keys are not compromised—then this factor would cut against finding harm. In those circumstances, it would be costly to decrypt the data, thus decreasing the risk that it could be used for criminal ends.

5. Missing Electronic Device with Personal Data.—Suppose a portable electronic device containing a plaintiff's personal data goes missing, and it is unknown whether the device was lost or stolen. This scenario is similar to the case above, although less is known. The device might just have been lost.[222]

In cases involving missing devices storing personal data, the evidence generally would not support a finding of a sufficient risk of future injury. This is especially true in cases involving personal data that alone or in combination with other data would not be considered sensitive—that is, data that can be cheaply and easily used to commit fraud. However, if the data on the device is embarrassing or highly sensitive, then there might be sufficient emotional distress harm in the mere exposure of this data to others. Anxiety over the risk—not of fraud but of the data being disclosed to others—can be sufficient for harm if it is reasonable to feel such anxiety based on the data involved. Of course, if the data is encrypted and the encryption keys are not compromised, then there would be no harm.

6. Personal Data Exposed Online.—Suppose a plaintiff's personal data is unwittingly exposed on the Internet for a period of time. Nothing is known about whether anyone saw or used the data. This case is similar to situations involving missing electronic devices with personal data. There generally will

222. This scenario is quite common. *See, e.g.*, Linda McGlasson, *Bank of New York Mellon Investigated for Lost Data Tape*, BANK INFO SECURITY (May 27, 2008), https://www.bankinfosecurity.com/bank-new-york-mellon-investigated-for-lost-data-tape-a-862 [https://perma.cc/2KFA-JU7T] (discussing the uncertainty as to whether missing tapes were lost or stolen).

not be enough evidence to demonstrate a sufficient risk of future injury, but there might be reasonable anxiety if the data is sensitive or embarrassing.

7. Personal Data Exposed in the Trash.—Suppose paper records with a plaintiff's personal data are thrown away in a dumpster. The records are all recovered, but it is unknown whether anyone accessed them while they were exposed in the dumpster.

The risk of future fraud and anxiety is lower here than the above examples. Unlike personal data posted online, paper records are more difficult to use than electronic data; the odds that criminals accessed the paper records, copied down the data, and left the records in the dumpster are low. The risk is especially small if the personal data is not sensitive.

What if the personal data is highly sensitive? What if the data includes medical records?[223] Given the low likelihood that such data was in fact discovered, anxiety about its misuse should be viewed as unreasonable. As a result, courts should not recognize risk and accompanying anxiety as cognizable harms.

8. Improper Access by an Organization's Employee.—Suppose an employee improperly accesses records concerning a plaintiff's personal data. Nothing is known about the use of the data.

The analysis will depend upon the nature of the data and what the likely motive of the employee was. A hospital employee snooping into a celebrity's medical record can cause reasonable anxiety because of the exposure of private health data. This is a classic example of intrusion upon seclusion and there would be emotional distress harm under that tort.

IV. Resisting Denial

Recognizing data-breach harms has significant downstream consequences in our legal system. Judicial reluctance to recognize harm might stem from a desire to avoid creating more opportunities for litigation, especially class-action lawsuits.

The law has various tools to provide redress for injuries, as well as to deter blameworthy conduct that leads to injuries. In data-breach cases, some of the most common tools include data-breach-notification laws, regulatory enforcement, and litigation. Data-breach-notification laws require provision of notice to people about data breaches,[224] but they do little to redress any injuries caused. The cost of sending out breach-notification letters can serve

223. This scenario has come up in state-attorney-general investigations. In such cases, AG offices have settled with pharmacies and medical practices for modest penalties and promises to undertake rigorous security measures. Citron, *supra* note 58, at 779 & n.211.

224. *Security Breach Notification Laws*, *supra* note 109.

as a deterrent, but these laws are often strict liability and are not tied to blameworthy conduct.[225] They thus do not deter the most blameworthy any more than the least blameworthy. Moreover, the cost of notification is not proportionate to the amount of harm that a breach might cause.

Regulatory enforcement can be effective, and the Federal Trade Commission (FTC), Federal Communications Commission (FCC), the Department of Health and Human Services (HHS), and state attorneys general, among others, have brought enforcement actions against organizations for data breaches.[226] Regulatory enforcement is limited in extensiveness, as regulatory agencies are only able to pursue a small number of cases. The FTC, for example, has brought only about sixty cases involving data security since 2002.[227] Moreover, individuals often have little say in whether enforcement actions are brought, and they lack much participation in the process. Regulatory enforcement waxes and wanes as agency priorities and personnel change. Not all state attorneys general vigorously enforce the regulation.

Private lawsuits serve a function that these other tools lack. Such lawsuits allow individuals to have a say about which cases are brought. These lawsuits bring out facts and information about blameworthy security practices by organizations. They provide redress to victims, and they act as a deterrent. But there are many flaws with litigation as a legal tool to deal with data breaches.

One concern is that runaway class actions could bankrupt companies. As one court noted, "for a court to require companies to pay damages to thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses."[228]

---

225. Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1146 (2009).

226. Citron, *supra* note 58, at 792–93, 799.

227. FED. TRADE COMM'N, PRIVACY & DATA SECURITY—UPDATE: 2016, at 4 (2016), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf [https://perma.cc/QE3Z-6B4D].

228. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015). However, harm might not necessarily lead to a dramatic increase in class action lawsuits. Under the current procedural rules, federal courts would not certify a class where individual issues of harm would predominate the case. *See* Alex Parkinson, Comment, *Comcast Corp. v. Behrend and Chaos on the Ground*, 81 U. CHI. L. REV. 1213, 1214, 1223–25 (2013) (interpreting *Comcast Corp. v. Behrend*, 133 S. Ct. 1426 (2013), to prohibit class certification where individualized damage questions predominate). Under both tests, context is an important consideration for the various factors. *See* Fed. R. Civ. P. 23(b)(3). This in turn may make it difficult to obtain certification for classes involving thousands of people. Consider a proposed class action in a case related to a data breach involving thousands of people's home addresses. Context is key to determining if the disclosure would raise the risk of physical harm and emotional distress. Individualized hearings would be necessary to determine whether the sharing of home address raised the risk of domestic abuse or stalking. In such a case, the description of the class would have to be carefully tailored to the data-breach harms to overcome challenges to certification.

One problem endemic to data breaches is one we will refer to as the "multiplier problem." This problem is caused by the fact that organizations can hold data on so many individuals that recognizing even a small amount of harm will be multiplied by a staggering number of people. These days, even a small company can have data on tens of millions of people. Judges are reluctant to recognize harm because it might mean bankrupting a company just to give each person a very tiny amount of compensation. Do we want bankruptcy-threatening liability for a data harm that only causes people a minor amount of harm?

The challenge with data breaches is that although the harm might be small to many people, it can add up as hundreds and perhaps thousands of organizations cumulatively cause harm to people. Moreover, a small amount of harm to many people might add up to more harm collectively than a large amount of harm to a few people.

Courts may also be concerned that class-action lawsuits for data breaches often do not provide much in the way of redress to individuals. These lawsuits can be slow, expensive, and punishing to the parties. Lawsuits can be so costly and time-consuming that organizations often settle just to avoid the pain of having the legal process resolve the case even when they think they will likely win.[229]

Despite these concerns, which are legitimate, courts should not focus on them when evaluating whether there is a legally cognizable harm. Courts should analyze whether the law should recognize harms independently from the downstream consequences of such recognition. Often, these downstream consequences become conflated with the issue of whether there should be legally cognizable harm. Harm should not be denied merely because finding harm will involve facing challenging issues about the form and amount of redress.

It is true that litigation is a flawed legal tool, but the other legal tools to deal with data breaches have limitations. New legal tools might work better. But none of these points should lead to failing to find harm. If there's a nail that needs to be hammered into the wall, and a hammer is not available, the solution is not to deny the existence of the nail. We reach this conclusion not just based on principle or a blind commitment to conceptual consistency, but on pragmatic grounds. At first blush, it generally does not seem pragmatic to argue that courts should recognize harm even though it could produce undesirable consequences in the legal system. But there are undesirable consequences for failing to recognize harm, which include allowing harm to

229. *See* Randy J. Kozel & David Rosenberg, *Solving the Nuisance-Value Settlement Problem: Mandatory Summary Judgment*, 90 VA. L. REV. 1849, 1850–51 (2004) ("The civil justice system is rife with situations in which the difference in cost between filing and ousting meritless claims or defenses makes the nuisance-value strategy profitable").

go undeterred. The consequences should be seen beyond the particular case. Data-breach harms in any one case might not be large for most individuals, but aggregated across many cases, the harms become much more significant.

Moreover, there are adverse consequences with conflating issues and not addressing each in an honest and direct manner. These consequences affect society's ability to grapple with problems of great social concern. Not recognizing data-breach harms is avoidant behavior that often leads to a poor response on two fronts. The first is that problems involving data-breach harms are not addressed. The second is that specific problems involving the way our legal system functions are ignored.

If there is a legally cognizable harm, then the law should try to address it. If the problem is that the forms of redress and remedies cause problems, then these problems should be grappled with directly rather than avoided. Suppose a person's job is to pick every apple on an apple tree. Some apples are high up in the tree and are difficult to pick. The person declares that they are not apples, so she does not have to pick them. This approach is not only dishonest—it is unproductive. A more honest and productive response would be to explore how to surmount the difficulties in picking them. Maybe a different method is needed. Maybe new tools can be created to pick the apples. Innovation and invention might lead to a solution, but this might never occur if the existence of the apples is denied.

Denying problems stunts the law's development and is one factor why the law struggles to respond rapidly and effectively to contemporary problems. A key reason why data-breach harms are not recognized as cognizable is because their recognition would push on many of the areas where the law is very gingerly developing. Some might argue that the law should turn away data-breach harms until it is fully prepared to embrace them. That view, however, ignores the expressive function of the law.[230] By rejecting data-breach harms, the law is saying that they are not worthy of redress. It is suggesting that they are not worth rethinking existing legal concepts or pushing harder on newer developing areas of the law. What originates in a lack of judicial imagination and fortitude becomes manifested in terms of data-breach harms being cast aside as insignificant or nonexistent.

It is difficult to set aside the law's current difficulties when tackling the question of whether the law should recognize data-breach harms. Bringing in the legal system with all its flaws might create negative outcomes. Shouldn't we consider the consequences of how our legal system will handle a certain matter?

The problem is that such an analysis takes the current legal system as fixed and unchangeable, and this is far from the case. The legal system will

230. *See* Citron, *supra* note 162, 376–77 ("[B]ecause law is expressive, it constructs our understanding of harms that are not trivial.").

never grow or mature if it is not challenged. The consequences might be worse in the short term, but this sacrifice might yield better results in the long term. Our legal system already has many different tools to redress harm, and has evolved considerably over the years.

Moreover, the existence of problems with the legal system cuts both ways in a consequentialist analysis. Part of the decision about whether to accept and live with something is how well it functions. If the legal system functions fairly well, then one might be more accepting of it. The further away the legal system is from acceptable, the stronger the argument for changing it. Thus, the worse the failings of our legal system, the better it is to push on it.

Additionally, denial of harm is not the only escape valve that the legal system can employ. Escape valves can be created at nearly any point in the process. Instead of addressing difficulties in how the legal system will handle cases when determining whether data harm exists, courts could address those difficulties and make compromises when actually addressing those cases. Rather than create a fiction that harm does not exist, why not create other fictions more directly on point and responsive to the problems for which they are being created?

Generally, those who cause wide-scale harm must pay for it. If a company builds a dam and it bursts and floods a town, that company must pay.[231] But with data-breach harms, courts are saying that companies should be off the hook and should not be made to internalize the harm. To the extent that there ought to be limits on liability for data harm, such limits are best addressed directly rather than through denying the existence of data-breach harm. For instance, not all harms might need to be addressed via damages and could be dealt with through various forms of equitable remedies and declaratory judgments.

The problems with our civil justice system and class actions exist in many other areas of law and for many other types of harm. Data-breach harms should not be singled out. To the extent the civil justice system is flawed, this is an issue that ought to be taken up systematically, most practically through our legislatures. It is not an excuse for courts to take it upon themselves to close off the civil justice system from redressing a serious and important type of harm.

Conclusion

Looking across the body of jurisprudence of data-breach harms, it is fair to say that courts are reluctant to recognize data-breach harms. Various lines

231. *See Reservoirs*, *supra* note 36, at 270–71 (analyzing data-breach cases as analogous to dam breach cases).

of cases that would support their recognition are ignored or narrowly interpreted. Courts rarely seize the opportunity to push doctrines in a progressive direction when it comes to data-breach harms. By contrast, courts are willing to extend the logic of related lines of cases in other contexts. Yet for data-breach harms, where precedent can be read flexibly and creatively, courts will rarely take the opportunity to do so. In many cases, courts brush aside or ignore precedent that would support the recognition of data-breach harms.

With a better understanding of harms, we can appreciate why they are harmful, why the law struggles, and why the law needs to do more. Although there are legitimate concerns with recognizing data-breach harms, not doing so is akin to being an ostrich hiding its head in the sand. The law offers a set of tools that can be used to address harm, from compensatory damages to equitable relief (such as injunctions) to remedies (such as unjust enrichment).

Our legal system needs to confront data-breach harms because real costs are borne by individuals and society and because ignoring them results in inefficient deterrence. Courts routinely avoid hard questions and ignore the anxiety people experience and the increased risk that data breaches cause. Yet in other areas of the law, courts have recognized such harms and placed manageable limits on their reach. As we have shown, those legal developments should inform how courts address data-breach harms. A path has been laid to help us work through the complexities of data-breach harms.

Data-breach harm might often be intangible, but it still is very real. Data harm is frequently risk-oriented, but risk management is a standard part of the way that the modern commercial world operates.

There are regulatory enforcement mechanisms to address harm, as well as many possibilities for legislation. What is the ideal mix of these tools? Are new tools needed? These are important questions to ask and ones we plan to address in future work. For now, though, it is important to note that these questions will not be asked sufficiently if no harm is recognized.

In this Article, we have attempted to lay the conceptual groundwork for understanding data-breach harms and to demonstrate the legal foundations that can be used to help the law grapple with data-breach harms. When the law fails to recognize harm, the costs of our data-driven society are externalized onto individuals. These costs are compounding as data-breach harms aggregate. Not recognizing data-breach harms can lead to under-deterrence of data security violations as well as inadequate investment in prevention. Dealing with data-breach harms will certainly be challenging, but the law is ready, and the stakes are of paramount importance.