RISK AND ANXIETY:
A THEORY OF DATA BREACH HARMS

by

Daniel J. Solove
Danielle Keats Citron

NOTE: This is a work-in-progress.
Please do not cite without permission.

RISK AND ANXIETY:
A THEORY OF DATA BREACH HARMS

Daniel J. Solove[1] and Danielle Keats Citron[2]

[1] John Marshall Harlan Research Professor of Law, George Washington University Law School. Thanks to Deven Desai, Will DeVries, Susan Freiwald, Chris Hoofnagle, Orin Kerr, Joel Reidenberg, 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.

[2] Lois K. Macht Research Professor & Professor of Law, University of Maryland Francis King Carey School of Law.

ABSTRACT

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 claims are viable. Plaintiffs have argued that data breaches create a risk of future injury from identity theft or fraud 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, resulting in a lack of consensus among courts and an incoherent jurisprudence.

In the past five years, the U.S. Supreme Court has contributed to this confounding state of affairs. 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 constitute "injury in fact" for standing. The Court emphasized that injury must be "certainly impending" to warrant recognition. This past term, the U.S. Supreme Court in* Spokeo v. Robins *issued an opinion aimed at clarifying the harm required for standing in a case involving personal data. But far from providing guidance, the opinion fostered greater confusion. What the Court made clear, however, was that "intangible" injury, including the "risk" of injury, could be sufficient to establish harm. In cases involving informational injuries, when is intangible injury like increased risk and anxiety "certainly impending" or "substantially likely to occur" to warrant standing? The answer is unclear.*

Little progress has been made to harmonize this troubled body of law, and there is no coherent theory or approach. In this essay, we examine why courts have struggled when dealing with 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. In many instances, courts should find that data breaches cause cognizable harm. We explore how existing legal foundations support the recognition of such harm. We demonstrate how courts can assess risk and anxiety in a concrete and coherent way.

INTRODUCTION

Suppose that Company X fails to adequately secure its clients' personal data. Imagine the company knows that hackers previously broke into its system yet did nothing about it. This time, hackers have little difficulty accessing the company's computer network and steal sensitive personal data about thousands of individuals. In the hackers' hands is now the key 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.[3] 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. 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 a defendant might have been with regard to security, no matter how much warning a defendant had about prior hacks and breaches, if plaintiffs cannot show harm, they cannot succeed in their lawsuit.

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 are deemed insufficient to warrant recognition of harm,[4] even though the law has evolved in other areas to redress such injuries.

[3] The issue of standing also comes up in state courts adjudicating data breach claims. See, e.g., Maglio v. Advocate Health, 40 NE3d 746, 752-753 (Ill. App. 2015) (explaining that federal standing principles are similar to those in Illinois and in turn dismissing data breach claims under Illinois law because risk of identity theft and emotional distress did not amount to injury in fact sufficient to support standing).

[4] *Compare* Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (finding that increased risk of identity theft is too speculative a harm in case involving the theft of personal data from payroll processing firm); Storm v. Paytime, Inc., No. 14-1138, 2015 WL 1119724, at *5-8 (M.D. Pa. Mar. 30, 2015) (same); Peters v. St. Joseph Servs. Corp., No. 14-2872, 2015 WL 589561, at *4-7, *8 (S.D. Tex. Feb. 11, 2015) (same); In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-347, 2014 WL 1858458, at *5-9, *14 (D.D.C. May 9, 2014) (same); Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 469-71 (D.N.J. 2013) (same) *with* Galaria v. Nationwide Mut. Ins., 2016 U.S. App. LEXIS 16840 (6th Cir. Sept. 16, 2016) (recognizing increased risk of identity theft and reasonably incurred mitigation costs to avoid future as harm warranting standing because hackers allegedly had stolen plaintiffs' information and defendant offered free credit monitoring services to help consumers mitigate danger); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Krottner v. Starbucks Corp., 628 F.2d 1139 (9th Cir. 2010); In Re Home Depot Customer Data Security Breach Litig., 2016 WL 2897520 (N.D. Ga. May 17, 2016) (finding harm to plaintiff financial institutions to

The courts' refusal to recognize data harms is, in no small part, due to confusion created by the Supreme Court decision in *Clapper v. Amnesty International*.[5] 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. 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. They spent significant money and time to protect the confidentiality of these communications, such as traveling abroad to speak with clients rather than talking to them on the phone.[6]

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). The Court acknowledged that the plaintiffs' theory of harm might be correct, but there was no proof that surveillance had, in fact, happened or was about to occur (or even that there was a substantial risk of it occurring in the future). The proof sought by the Court was absent because, according to the government, the surveillance program had to be kept secret. Thus, because 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. The Court held that plaintiffs lacked standing to sue because they could not show that the actual injury of government surveillance was underway or "certainly impending." The plaintiffs' case was dismissed because the plaintiffs could only speculate about whether their communications were under surveillance.[7]

Although the *Clapper* Court focused on the fact that plaintiffs could not show that government surveillance was imminent or certainly impending, it stated in a footnote that, "in some instances," a "substantial risk that the harm will occur would be sufficient to confer standing to plaintiff."[8] The Court failed to elaborate more on this point.

---

warrant standing in case concerning hackers' breach of Home Depot's databases for costs undertaken to avoid future harm including costs to cancel and reissue cards, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and fees due to reduced card usage).

[5] 133 S. Ct. 1138 (2013).

[6] For a thoughtful analysis of Clapper, *see* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

[7] The *Clapper* case comes with a dose of cruel irony. Although the government diminished the plaintiffs' concerns about surveillance by arguing that the plaintiffs could not prove that they were subject to it, the government knew the answer all along, but because the program was classified as a state secret, the plaintiffs did not and could not know for sure that they were being subject to surveillance. See Seth F. Kreimer, *"Spooky Action at a Distance:" Intangible Injury in Fact in the Information Age*, 18 U PA. J. CON. L. 745, 757 (2016).

[8] *Id.* at 1150 n.5. In *Susan B. Anthony List v. Driehaus*, the Court, quoting *Clapper*, held that "an allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." 134 S. Ct. 2334, 2341 (2014).

In decision after decision, courts have relied on *Clapper* to dismiss data breach cases. For example, in *Reilly v. Ceridian Corp.*,[9] the case on 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." 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."[10] Because thieves had not yet misused the plaintiffs' data, there was no "actual" harm to warrant standing or redress.[11] The court summarily rejected the plaintiffs' claims of emotional distress.

Much like *Reilly*, the majority of courts have ruled that injuries from data breaches are too speculative and hypothetical, too based on subjective fears and anxieties, and not concrete and significant enough to warrant recognition.[12] Courts have held that the "mere increased risk of identity theft or identity fraud alone does not constitute a cognizable injury."[13] 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.[14] 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.

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. In those cases, plaintiffs were found to have suffered actual, and not hypothetical, injuries where hackers stole personal data from inadequately secured systems.[15] In *Remijas v. Neiman Marcus Group, LLC*, the

[9] 664 F.3d 38 (3d Cir. 2011).
[10] *Id.* at 42.
[11] *Id.* at 43.
[12] See, e.g., In re Horizon Healthcare Servs., Inc. Data Breach Litig., No. 13-7418, 2015 WL 1472483 (D. N.J. Mar. 31, 2015); Peters v. St. Joseph Servs. Corp., F.Supp.3d, 2015 WL 589561 (S.D. Tex. Feb. 11, 2015); Storm v. Paytime, Inc., F.Supp.3d, 2015 WL 1119724 (M.D. Pa. Mar. 13, 2015).
[13] Green v. eBay Inc., --F.3d.3d--, 2015 WL 2066531 (E.D. La. May 4, 2015).
[14] See, e.g., Bradix v. Advance Stores Co., Inc., 2016 WL 3617717 (E.D. La. July 6, 2016) (dismissing claims for lack of injury in fact in case where plaintiff alleged that defendant's employee gave hacker employees' names, Social Security Numbers, gross wages, and state where employees pay income taxes and that information was used in unauthorized attempts to secure vehicle financing appearing on plaintiff's credit report because there was no proof that the attempts at fraud damaged plaintiff's credit score); Alleruzzo v. Supervalu, Inc., 2016 WL 1588105 (April 20, 2016) (finding no harm to support standing even though plaintiffs alleged malicious software released and disclosed payment card names and PINs because the only alleged misuse of personal data was single unauthorized charge on one plaintiff's credit card).
[15] Galaria v. Nationwide Mutual Insur. Co., 2016 WL 4728027 (6th Cir. 2016) (finding substantial risk of harm, coupled with reasonably incurred mitigation costs, supported standing in data breach case because theft of personal data by ill-intentioned criminals placed them at continuing, increased risk of fraud and identity theft and plaintiff suffered three unauthorized attempts to open credit cards in his name); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693-94 (7th Cir. 2015) (finding that 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 v. Starbucks, Corp., 628 F.3d 1139 (9th Cir. 2010) (finding increased risk of identity theft constituted injury in fact where given that someone had attempted to use stolen personal

Seventh Circuit reasoned, "Why else would hackers break into a store's database and steal consumers' personal information? Presumably, the purpose of the hack is, sooner or later, to make a fraudulent charge or assume those consumers' identities."[16] Trial 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.[17]

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 v. Robins*[18] 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 defendant, a "people search engine," violated the federal Fair Credit Reporting Act (FCRA) when it published false information about him. The defendant's dossier asserted that plaintiff was wealthy, married with children, and worked in a professional field though he was none of those things. Plaintiff alleged that the inaccuracies in defendant's dossier damaged his employment chances by suggesting that he was overqualified or that he might be unwilling to relocate because of responsibilities to his non-existent family. The district court found that the plaintiff lacked standing to sue under Article III because the alleged injury—defendant's publication of inaccurate information—was too abstract.

After the Ninth Circuit reinstated the plaintiff's case on the grounds that an inaccurate credit report amounted to a particularized injury sufficient to support standing, the Supreme Court granted the defendant's writ for certiorari. 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 "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."

---

data to open 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. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157-59 (D. Minn. 2014) (finding that unlawful charges, restricted or blocked access to bank accounts, inability to pay bills, and late payment charges or new card fees incurred by plaintiffs constituted injuries in fact in the wake of the theft of credit card and personal data of 110 million customers).

[16] *Remijas*, 794 F.3d at 693.

[17]

[18]

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. Although this issue is at the heart of data breach cases, it has received little sustained scholarly attention.[19] Debates about data breach harms rarely delve into the muddy conceptual waters. 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.

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. Because companies do not have to internalize the negative externalities borne by individuals, the number of data breaches continues to grow. 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 towards 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; 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. Sufficient foundations in law exist for courts to assess increased risk of harm in data breach cases.

[19] Ryan Calo has done important work on privacy harms, setting out a theoretical framework to assess the boundaries of privacy harm. Ryan M. Calo, *The Boundaries of Privacy Harms*, IND. L. J. (2009). Under his account, the boundaries of privacy harms can be distilled to objective harms and subjective harms. Calo's theoretical contributions are instructive to ours, though we look to historical common law doctrines for the foundation of data harms that can be recognized by courts.

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. In other contexts, however, courts routinely accept various forms of emotional distress, including anxiety, as sufficient harm. Indeed, in some areas, the issue of harm is not even discussed in most cases and is rarely an issue on appeal.[20] For example, the privacy torts, recognized in the vast majority of states, allow plaintiffs to recover for disclosure of private information or for the improper intrusion into private matters resulting in emotional distress if the defendant's conduct is "highly offensive to the reasonable person." [21] The tort of breach of confidentiality recognizes emotional distress as a cognizable injury without the need to show highly offensive conduct.[22]

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

This Article has three parts. Part I discusses 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 HARMS

Harm is indispensable to most private law claims. Generally speaking, "harm" is understood as the impairment, or set back, of a person, entity, or society's interests.[24] People or entities suffer harm if they are in worse shape than they would be had the activity not occurred.[25] Harm frustrates a person' ability to "fashion a life . . . that is

[20] *See infra* Part II.B.2
[21] *See infra* Part II.B.2
[22] *See infra* Part II.B.2
[23] *See infra* Part II.A.3
[24] 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.*
[25] Joel Feinberg, *Wrongful Life and the Counterfactual Element in Harming*, in FREEDOM AND FULFILLMENT 3 (1992); Stephen Perry, *Harm, History, and* Counterfactuals, 40 SAN DIEGO L. REV.

distinctively and authentically hers."[26] Harms 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."[27]

A "legally cognizable harm" is harm that the law recognizes as worthy of redress, deterrence, or punishment.[28] Reasonable foreseeability of harm is a fundamental principle of much of private law.[29] 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 against which tort law was directed.[30] 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.[31] To be sure, legislation sometimes permits statutory damages or includes liquated damages provisions, which permit redress without additional showings of harm.[32] The harm is understood as the interference with the right recognized in the statute, so long as the plaintiff has suffered some set back to tangible or intangible interests.[33] .

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."[34] The injury must be "concrete and particularized" and "actual or imminent, not conjectural or

1283, 1292 (2003) (exploring concepts of harm understood as interest with someone's interest in a way that makes them historically worse off).

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

[27] JOEL FEINBERG, HARM TO OTHERS: THE MORAL LIMITS OF CRIMINAL LAW 37 (1984).

[28] As Joel Feinberg explains, harms may involve invasions or setbacks to interests but not all invasions of interests are worthy of law's attention. JOEL FEINBERG, HARM TO OTHERS: THE MORAL LIMITS OF CRIMINAL LAW 34 (1984). 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*. at 34-35.

[29] Gregory Keating, *When is Emotional Distress Harm?*, in TORT LAW: CHALLENGING ORTHODOXY 299 n. 89, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2460072.

[30] Oliver Wendell Holmes, THE COMMON LAW 64 (1881, reissued 1963); see Thomas C. Grey, *Accidental Torts*, 54 VAND. L. REV. 1225, 1272 (2001) (exploring Holmes's harm-based approach).

[31] 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.

[32] Copyright law is a prime example of statutory damages without harm.

[33] Spokeo v. Robins. Some statutes like the Privacy Act of 1974 require an additional showing of harm for individuals to bring suit. NASA v. Nelson. 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, NOTRE DAME L. REV. (forthcoming 2017). Because private UDAP claims require a showing of harm—whether or not statutes so require, courts routinely dismiss them.

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

hypothetical."[35] If a plaintiff lacks standing to bring a claim, a federal court cannot hear it.

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 think about data breach cases, most often resulting in their dismissal early in the litigation. Courts have found a lack of an "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 analysis of security risks.[36] The Ashley Madison breach released information about people's extramarital affairs.[37] The Sony breach involved employee email.[38] The Target breach resulted in the leaking of credit card information, bank account numbers, and other financial data. 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. 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). In a study of 230 data breach lawsuits between 2004 and 2014, plaintiffs brought more than 86 different causes of action.[39]

[35] *Id.*

[36] Kim Zetter and 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/; http://www.wired.com/2015/07/massive-opm-hack-actually-affected-25-million/.

[37] Danielle Keats Citron & Maram Salaheldin, *Leave Cheaters in Peace*, N.Y. DAILY NEWS, August 24, 2015, http://www.nydailynews.com/opinion/citron-salaheldin-leave-cheaters-peace-article-1.2333852.

[38] Kim Zetter, *Sony Got Hacked Hard*, WIRED, http://www.wired.com/2014/12/sony-hack-what-we-know/.

[39] Sasha Romanosky, David A. Hoffman, and Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 JOURNAL OF EMPIRICAL LEGAL STUDIES 74 (2014).

Data breach cases are often filed in federal court or removed there from state court under the federal Class Action Fairness Act (CAFA).[40] Under CAFA, class actions can be removed to federal court for state law claims exceeding five million dollars where at least one member of the putative class and one defendant reside in different states.[41] 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 the personal data.[42] Courts view the increased risk of identity theft not as an "actual injury" but rather as "speculation of future harm."[43]

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.[44] In a case where plaintiffs' sensitive financial data was accessed 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.[45] Because hackers had not opened new bank accounts or credit cards in plaintiffs' names, there was no harm.[46] This was true in *Key v. DSW*,

[40] Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d).
[41] *Id.*
[42] See, e.g., Forbes v. Wells Fargo Bank, 420 F. Supp.2d 1018 (D. Minn. 2008) (granting defendant's motion for summary judgment in case involving the theft of personal data from defendant's system because there was no indication that the information on the stolen computers had been misused); Guin v. Higher Educ. Serv. Corp., Inc., 2006 WL 288483 (D. Minn. 2006).
[43] In re Barnes & Noble Pin Pad Litig., 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013); Hammer v. Sam's East, Inc., 2013 WL 3746573 (D. Kan. July 16, 2013) (explaining that "[n]o court has found that a mere increased risk of ID theft or fraud constitutes an injury in fact for standing purposes without some alleged theft of personal data or security breach").
[44] *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); Hammond v. Bank of New York, 2010 WL 2643307 (S.D.N.Y. June 25, 2010); Bell v. Acxiom Corp., 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (dismissing negligence claim in case involving hacking of defendant's databases storing plaintiffs' personal data because being at higher risk for fraud is insufficient harm to warrant standing).
[45] Storm v. Paytime, Inc., 90 F. Supp.3d 359, 366 (M.D. Pa. 2015).
[46] *Id.* at 367.

Inc.,[47] where thieves gained access to the defendant shoe retailer's computer system containing the financial data of 96,000 customers.[48] The court found no harm because plaintiffs only alleged the possibility of being victimized "at some unidentified point in the indefinite future."[49]

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.[50] In *Fernandez v. Leidos, Inc.*,[51] for instance, the district court dismissed plaintiff's increased risk of harm in the wake of the theft of backup tapes with his personal data because the capabilities and criminal intentions of data thieves were speculative.[52] Even when plaintiffs quantify the extent to which the data breach has elevated their risk of future harm, courts still find that the harm too speculative to proceed.[53] In *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*,[54] the plaintiffs argued that they were nearly ten times more likely to be victimized by identity theft. 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." Another court sharpened the point, reasoning that identity theft was unlikely to happen in the future since the plaintiffs had not experienced fraud in the year after the breach.[55]

Although three Courts of Appeal have recognized increased risk of harm as cognizable, these cases involved allegations about the malicious purpose of hackers and actual or attempted misuses of leaked personal data. In *Remijas v. Neiman Marcus Group*, 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."[56] Moreover, the defendant "contacted members of the class to tell them they were at risk," which the court viewed as an admission that plaintiffs had suffered non-speculative harm.[57] In *Krottner v. Starbucks Corp.,* the Ninth

[47] 454 F. Supp.2d 684 (S.D. Ohio 2006).
[48] *Id*. at 686.
[49] Id. at 690. *See also* Bell v. Acxiom Corp., 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (dismissing negligence claim in case involving hacking of defendant's databases storing plaintiffs' personal data because being at higher risk for fraud is insufficient harm to warrant standing);
[50] Reilly v. Ceridian Corp., 664 F.3d 38, 42-43 (3d Cir. 2011).
[51] 127 F. Supp.3d 1078 (E.D. Cal. 2015).
[52] Fernandez, 127 F. Supp.3d at 1087,
[53] Storm, 90 F. Supp.3d at 367.
[54] No. MDL 2360, 2014 U.S. Dist. LEXIS 64125 (D.D.C. May 9, 2014).
[55] Paytime, 90 F. Supp.3d at 367.
[56] See Remijas v. Neiman Marcus Group (7th Cir. 2015), http://cases.justia.com/federal/appellate-courts/ca7/14-3122/14-3122-2015-07-20.pdf?ts=1437415269; Danielle Keats Citron, *Some Good News for Data Breach Plaintiffs, 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/.
[57] Remijas; Lewart v. PF Chang's, No. 14-3700, at 6 (7th Cir. April 16, 2016) (recognizing future risk of harm sufficient to recognize standing where hackers stole personal data from retailer). The Sixth Circuit's recent decision in *Galaria* similarly pointed to the defendant's provision of credit monitoring as supporting increased risk of harm.

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.[58]

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.[59]

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; they have to 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 an attempt to "manufacture" injury.[60]

The preventative measure theory of harm typically fails because it is based upon the increased risk of future injury theory. 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, in turn creating 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 all the time. As a federal district court in New Jersey noted, courts "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 would be used in a malicious way.[61]

[58] 628 F.3d 1139 (9th Cir. 2010).
[59] *See*, *e.g.*, Forbes v. Wells Fargo Bank, 420 F. Supp.2d 1018 (D. Minn. 2008) and other cases discussed in notes 31 through 39.
[60] See, e.g., Polanco v. Omnicell, Inc. (D. N.J. Dec. 26, 2013).
[61] Crisafulli v. Ameritias Life Insur. Co., 2015 WL 1969173, at *4 (D. N.J. 2015).

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 suggesting emotional injury."[62] One court stated, "even if [the risk of identity theft] is enough to engender some anxiety" and "even if their fears are rational," plaintiffs lack standing "based on risk alone."[63] As another court concluded: "Emotional distress in the wake of a security breach is insufficient to establish standing."[64] 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.[65] Most courts consider plaintiffs' fear, anxiety, and psychic distress about their increased risk of identity theft and other abuses "too remote" to warrant recognition.[66]

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 harms be visceral—easy to see, measure, and quantify. 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.

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.[67] Financial losses could be recovered in tort actions if defendants owed plaintiffs a special duty of care.[68] Along these lines, courts have recognized claims for privacy violations only where redress is sought for tangible financial losses.[69] Courts have found a sufficient injury in data breach cases where the exposure of

[62] Crisafulli v. Ameritas Life Insurance Co., No. 13-5937, 2015 WL 1969176 (D.N.J. Apr. 30, 2015).
[63] Science Applications International Corp. Backup Tape Data Theft Litigation, 45 F.Supp.3d 14, 26 (D.D.C. 2014); see also Maglio v. Advocate Health & Hosps., 49 N.E.3d 746, 755 (Ill. App. 2015).
[64] In Re Barnes & Noble Pin Pad Litigation, No. 12-cv-8617, 2013 WL 4759588, at *5 (N.D. Ill. 2013).
[65] *Id.*
[66] Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009).
[67] Gregory C. Keating, *The Priority of Respect Over Repair*, 18 LEGAL THEORY J. 293, 313 (2013).
[68] The economic loss rule does not apply when defendant owe plaintiffs a special duty of care.
[69] Fraley v. Facebook, 830 F. Supp.2d 785 (N.D. Cal. 2011).

personal data has led to identity theft.[70] But without proof of physical harm or financial loss, courts rarely recognize harm.[71]

Requiring harm to be visceral and vested has severely restricted the recognition of data 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 legislative activity. 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? Why would the Federal Trade Commission and state attorneys general devote considerable time and resources pursuing data breach cases?[72] 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 they should evolve to do so in context of data breach harms.

---

[70] Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012). 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 experienced by identity theft victims: the entities that leaked the data, the companies that allow thieves to open up accounts in victims' names, and the credit reporting agencies that assemble the faulty information and use it to report on people's reputations. Chris Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J. L. TECH. 1 (2009). When victims attempt to clean up their credit reports, they are often prevented from doing so by uncooperative credit reporting agencies and creditors. http://www.nytimes.com/2015/03/10/business/big-credit-reporting-agencies-to-overhaul-error-fixing-process.html?_r=0

[71] In Re Hannaford Bros. Co. Customer Data Security Breach Litigation, 4 A.3d 492 (Sup. Ct. Me. 2010).

[72] See Citron, *State Attorneys General*, *supra* note.

II. RISK AND ANXIETY AS HARMS

The nature of data breach harms is a complex issue that has not been accorded adequate consideration in cursory judicial explanations. In this Part, we explore why courts are struggling 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 significant 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. Fraud may not surface until after 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? Years after personal data is leaked, identity theft victims have faced financial ruin. Identity thieves plunder people's credit, riddling their credit reports with false information including debts and second mortgages obtained in their names. Victims struggling with identity theft have been forced to file for bankruptcy, and some have lost their homes.[73] Victims are turned down for loans or end up paying higher interest rates on credit cards.[74] Their utilities are cut off and their services denied.[75] Identity thieves can use stolen health information to obtain medical care, saddling individuals with hefty hospital bills and a thief's treatment records.[76] Victims 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 three hundred dollars.[77] On average, it takes up to thirty hours to resolve problems when

[73] http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/

[74] Bureau of Justice Statistics, "Victims of Identity Theft, 2012," December 2013, at 7 http://www.bjs.gov/content/pub/pdf/vit12.pdf.

[75] http://www.bjs.gov/content/pub/pdf/vit12.pdf.

[76] Citron, *Reservoirs*, supra note.

[77] Bureau of Justice Statistics, "Victims of Identity Theft, 2012," December 2013, at 6, http://www.bjs.gov/content/pub/pdf/vit12.pdf.

identity thieves open new accounts in victims' names.[78] To be sure, some types of data 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.[79]

The problem with identity theft is that personal data cannot readily be "cancelled" or changed 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 changed. Biometric data such as fingerprints or eye scans, health information, and genetic data cannot be exchanged or cancelled. 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.

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."[80] Similarly, Ed Mierzwinski, the federal Consumer Program Director and Senior Fellow for U.S. PIRG, notes:

> 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 Numbers 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.

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

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.[81] 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.

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. The 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.

---

[78] *Id*. at 10.

[79] Andrea Peterson, *Data Exposed in Breaches Can Follow People Forever*, 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/

[80] *Id.*

[81] Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, in SECURING PRIVACY IN THE INTERNET AGE 112 (Anupam Chander, Lauren Gelman, and Margaret Jane Radin, eds. 2008).

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. State attorneys general often insist that companies pay consumers one to two years of credit monitoring and identity theft insurance after a security breach.[82]

Another component of the data breach harm involves a chilling of a person's ability to engage in life's important activities. An increased risk of identity theft might prevent a person 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 put at risk 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, and 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.[83] 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 difficult to obtain a new one. Then too, a person might be chilled from seeking a job that requires a security clearance.

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.

[82] Press Release, AG Jepsen to Anthem: End Unreasonable Delays in Providing Information to Affected Residents, February 10, 2015 http://www.ct.gov/ag/cwp/view.asp?Q=560660&A=2341 (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).

[83] Consumers Union, *Big Three Credit Bureaus Settle with 31 States Over Credit Reporting Mistakes*, May 26, 2015, http://consumersunion.org/2015/05/big-3-credit-bureaus-settle-with-31-states-over-credit-reporting-mistakes/ (explaining that one in five consumers have an error in credit reports).

Does a future risk of injury constitute real harm? It might be hard to see, but 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."[84]

People have a meaningful interest in avoiding risk.[85] 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 recognize risk as a cognizable harm in data breach cases. Risk is a central concept toward making more intelligent and practical decisions. As Justice

[84] David A. Fischer, *Tort Recovery for a Loss of a Chance*, 36 WAKE L. REV. 605, 633 (2001). See Zehner v. Post Oak Oil Co., 640 P.2d 991 (Oakl. Ct. App. 1981) (allowing 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).

[85] Levit, *supra* note, at 181.

Oliver Wendell Holmes famously observed, "the man of the future is the man of statistics and the master of economics."[86] 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 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.[87] Over time, probabilistic injuries have been recognized in three conceptually related areas: increased risk of injury, loss of a chance, and fear of disease.[88] 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.[89] For these claims, the harm is the destruction of a future opportunity and the loss of hope.[90]

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."[91] Under risk of future harm cases, damages include those "directly resulting 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."[92] For example, in *Petriello v. Kalman*,[93] a physician made an error that damaged the plaintiff's intestines. The plaintiff was estimated to have between an 8% to 16% chance that she would suffer a future bowel obstruction. 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."[94]

---

[86] OLIVER WENDELL HOLMES, *The Path Of The Law*, *in* COLLECTED LEGAL PAPERS 167, 187 (1920).
[87] Levit, *supra* note, at 154.
[88] *Id*. at 154.
[89] *Id.* at 155.
[90] *Id*. at 158.
[91] Lord v. Lovett, 770 A.3d 1103 (N.H. 2001). *See* Claire Finkelstein, *Is Risk a Harm?*, 151 U. PA. L. REV. 963, 970-90 (2003).
[92] Joseph H. King, Jr., *"Reduction of Likelihood" Reformulation and Other Retrofitting of the Loss-of-Chance Doctrine*, 28 U. MEM. L. REV. 491, 502 (1998).
[93] 576 A.2d 474 (Conn. 1990).
[94] *Id.*

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."[95] Courts have found increased risk of disease sufficient for standing purposes and as the basis of regulation.[96]

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 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 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.[97] 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, and the excess risk of fraud is certain to take its toll on a number of those users. Over time, the risk 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,

[95] Albert C. Lin, *The Unifying Role of Harm in Environmental Law*, 2006 WISC. L. REV. 897, 908 (2006).

[96] Due Power Co. v. Carolina Envtl. Study Grp., 438 U.S. 59, 74 (1974); Ethyl Corp. v. EPA, 541 F.2d 1 (D.C. Cir. 1976).

[97] See Rosenberg, *supra* note, at 883 (arguing that increased risk due to exposure to toxic materials is not negligence in the air but real harm due to excessive risk of diseased that is certain to take its toll on a percentage of those exposed).

recognized in common law, can provide the basis for harm sufficient to support standing. 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. Statute of limitations would likely bar any lawsuit. Even if statute of limitations is not a bar, delay in resolving the issue may lead to the loss of evidence.

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 temerity 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. With a data breach, anxiety is experienced in the present, but courts are reluctant to recognize emotional distress as a cognizable injury arising out of data breach harms.

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 statements 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, 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.

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, 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. 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 does 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. 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 use her computer to send out spam.

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 feelings 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, a reality that demonstrates that data breaches are not a trivial matter to legislatures. The media often report on data breaches, 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. They are told to shred documents with sensitive personal data and

to avoid carrying such data around in their wallets. 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 many laws and 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. 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 policymakers 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 too ethereal, too difficult to measure, too easy to fake.[98] That view of emotional distress faded in the mid-twentieth century. 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.[99] In some instances, the recognition of emotional distress traces its roots back before the modern era. The intentional tort of assault redressed emotional distress without any showing of physical injury.[100] Relational torts like the alienation of affection, of a similar vintage, permitted compensation for emotional distress.[101]

Privacy law's roots supported the recognition of emotional distress as a compensable injury in the early twentieth century. In *The Right to Privacy*,[102] Samuel Warren and Louis Brandeis spent considerable energy discussing the evolving nature of harm, from tangible to intangible injuries. "[I]n early times," they contended, "the law gave a remedy only for physical interference with life and property."[103] 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

[98] Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 172 (1992); Leslie Benton Sander & Carol Berry, *Recovery for Negligent Infliction of Emotional Distress Attendant to Economic Loss: A Reassessment*, 37 ARIZ. L. REV. 1247, 1253-59 (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. Rodrigues v. State, 472 P.2d 509, 520 (Haw. 1970); *see also* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. (2009). 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. Amanda Pustilnik, *Imaging Brains, Changing Minds: How Pain Neuroimaging Can Inform the Law*, 66 ALA. L. REV. (2015).

[99] Levit, *supra* note, at 158.

[100] Robert Rabin, *Emotional Distress in Tort Law: Themes of Constraint*," 44 Wake Forest L. Rev. 1197, 1197 (2009).

[101] *Id.*

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

[103] *Id.* at 193.

offensive noises and odors, against dust and smoke, and excessive vibration. The law of nuisance was developed."[104] Property developed to include "every form of possession—intangible, as well as tangible."[105] 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.[106]

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 involved an "injury to the feelings."[107] Warren and Brandeis identified the legally protected interest set back by privacy invasions as a person's ability to develop her "inviolate" personality.[108] Privacy invasions inflicted 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 interfered with a person's "estimate of himself," inflicting "mental pain and distress, far greater than could be inflicted by mere bodily injury."[109]

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.[110] Courts recognized that emotional distress could be "as severe and debilitating as physical harm."[111] Privacy tort claims have succeeded in garnering compensation for emotional distress.[112] Plaintiffs have prevailed in cases involving the dissemination of nude photos,[113] before and after photos of plastic surgery patients,[114] and autopsy or death scene photos of loved ones.[115] Courts do not

[104] *Id*. at 194.
[105] *Id*. at 193.
[106] Restatement (Second) of Torts § 623 (1977). Defamation liability includes redress for emotional distress caused by the defamatory publication. *Id.*
[107] *Id.* at 197.
[108] *Id.* at 196.
[109] *Id*.
[110] Calvert Magruder, *Mental and Emotional Disturbance in the Law of Torts*, 49 HARV. L. REV. 1033 (1936).
[111] Molien v. Kaiser Foundation Hosp., 167 Cal. Rptr. 831, 832 (1980).
[112] *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1811-14 (2010) (exploring privacy tort cases awarding damages for emotional distress, mental anguish, worry, and embarrassment).
[113] Daily Times Democrat v. Graham, 162 So.2d 474, 476 (Ala. 1964) (awarding damages for embarrassment and humiliation after newspaper published a picture of 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 (June 13, 2012) (awarding plaintiff damages for intentional infliction of emotional distress and public disclosure of private fact where defendant posted her intimate photographs online, e-mailed them to her husband, and created fake Twitter accounts displaying them).
[114] Vassiliades v. Garfinkle's, 492 A.2d 580, 586 (D.C. 1985).
[115] *See* Catsouras v. Dep't of the California Highway Patrol (CHP), 104 Cal. Rptr. 3d 352 (2010); Douglas v. Stokes, 149 S.W. 849, 850 (Ky. 1912). 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* National Archives and Records Admin. v. Favish, 541 U.S. 157 (2004) ("Family members have a personal stake in honoring and mourning their

question the harm in those cases, even though it involves intangible injury.[116] 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.[117]

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."[118] Elder explains that courts have permitted harms such as "injury to feelings or sensibilities; feelings of violation and mortification; fear for physical security; . . . past or future humiliation; [and] embarrassment," among other things.[119] According to the Restatement of Torts, plaintiffs can recover for purely emotional distress harm.[120] As one court put it, plaintiffs are "entitled to recover substantial damages, although the only damages suffered resulted from mental anguish."[121]

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 to the body."[122] As a court noted: "The difficulty of measuring damages for invasion of privacy is no reason for denying relief."[123] 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 worth and importance,' for emotional distress without any proof of special damages or physical or otherwise debilitating psychic injury."[124]

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."[125] 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

---

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.").

[116] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007).

[117] Catsouras, 104 Cal. Rptr. 3d at 355; Stokes, 149 S.W. at 850.

[118] DAVID. A. ELDER, PRIVACY TORTS §3-8 at p. 3-89.

[119] Elder 3:8 3-90 to 3-92.

[120] Restatement (Second) of Torts 652H comm. b.

[121] Brents v. Morgan, 299 SW 967, 971 (Ky 1927).

[122] Gonzales v. Southwestern Bell Tel Co., 555 SW2d 219, 222 (Tex Civ. App. 1977).

[123] Socialist Workers Party v. Attorney General, 642 F. Supp. 1357 1420-33.

[124] DAVID. A. ELDER, PRIVACY TORTS §2-10 at p.

[125] *Id*. See Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2009).

professional relationships. As Elder notes, the "permissible damages are broad and parallel those available under the intrusion and other privacy torts."[126] Additionally, in other contexts, courts accept emotional distress damages based solely upon the plaintiff's testimony, such as in employment discrimination cases.[127]

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.[128] Humiliation, nervousness, worry, and loss of sleep are understood as compensable harms.[129]

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.[130] Claims for negligent infliction of emotional distress initially were limited to cases involving physical injury, but that rule eased over time. 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."[131] Courts have recognized negligent infliction of emotional distress claims where the emotional distress occurs in the context of relationships that impose independent, pre-existing duties of care.[132]

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.[133] For example, in *Johnson v. West Virginia University*

[126] David A. Elder, *Privacy Torts*, §5:2 5-28 to 531.

[127] 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.").

[128] Citron, *Mainstreaming*, supra note, at 1811-14.

[129] *Id.*

[130] Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CAL. L. REV. 772, 773 (1985).

[131] Levit, *supra* note, at 144.

[132] Keating, *When is Emotional Distress Harm*, *supra* note, at 278.

[133] *Emotional Distress Damages for Fear of Contracting AIDS: Should Plaintiffs Have to Show Exposure to HIV?*, 99 DICKINSON L. REV. 779, 794 (1995); Note, *Can HIV-Negative Plaintiffs Recover Emotional Distress Damages for Their Fear of AIDS?*, 62 FORDHAM L. REV. 225, 237-39 (1993).

Hospitals,[134] the court held that a security guard could sue for emotional distress caused by the fear of contracting AIDS after being bitten by an AIDS patient. Although a majority of courts require plaintiffs to prove actual exposure to HIV,[135] a number of courts do not require exposure to HIV to warrant recovery for emotional distress.[136] Courts have also permitted emotional distress damages based on fear of contracting cancer. In one case, a court held that the plaintiff's fear of getting cancer after being exposed to asbestos was reasonable and actionable.[137]

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, 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.[138] These bodies of law have laid the

[134] 413 *S.E.*2d 889, 892-95 (W. Va. 1991).

[135] Majca v. Beekil, 701 N.E.2d 1084 (Ill. 1998) ("[A] 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 by *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., 186 W. Va. 648, 413 S.E.2d 889 (1991); Neal v. Neal, 125 Idaho 617, 873 P.2d 871 (1994) (requiring actual exposure to a sexually transmitted disease including HIV).

[136] See Williamson v. Waldman, 150 N.J. 232, 696 A.2d 14 (1997); Hartwig v. Oregon Trail Eye Clinic, 254 Neb. 777 (1998); Madrid v. Lincoln County Medical Center, 923 P.2d 1154 (N.M.1996); Faya v. Almaraz, 329 Md. 435, 620 A.2d 327 (1993); see also Marchica v. Long Island R.R. Co., 31 F.3d 1197 (2d Cir. 1994).

[137] Devlin v. Johns-Manville Corp., 202 N.J. Super. 556, 561, 495 *A.*2d 495 (Law Div.1985)

[138] 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." RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL & EMOTIONAL HARM (TENTATIVE DRAFT No. 5) (2007) at xxi. The Reporters Memorandum recognizes that the restrictions are arbitrary but that "given the ubiquity of emotional disturbances, lines must be drawn." *Id.*

foundation to extend emotional distress damages to cases involving inadequate security.[139]

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 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 to 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 and 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.[140] On the other hand, if a thief steals a car with

[139] *See generally* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805 (2010); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).
[140] *Adobe*, 66 F. Supp.3d at 1206-08.

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 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 drivers' 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. 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 readily be combined with data to cause harm to individuals. It is nearly impossible to figure out in advance all the possible 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 fraudulent charges, many major credit card companies have a zero-fraud liability policy.[141] Thus, where reasonable costs are likely to be reimbursed, this should be considered in 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 cost 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

[141] Whalen v. Michael Stores, Inc., 153 F. Supp.3d 577 (E.D.N.Y. 2015) (finding no harm in data breach case involving hack of credit card numbers because plaintiff would not have suffered liability for unauthorized charges after data breach and because she cancelled her credit card).

the problem of the overly-sensitive 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. But there are ways to distinguish genuine measures from manufactured ones. The key issue that the Court should have analyzed in *Capper* 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 nearly 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.[142]

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 person."[143] Intentional infliction of emotional distress claims can succeed only if plaintiffs can show that their anxiety was caused by "severe and outrageous" conduct.[144] 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

[142] Troy Hunt, "Here's What Ashley Madison Members Have Said to Me," Troy Hunt Blog, https://www.troyhunt.com/heres-what-ashley-madison-members-have/.
[143] Citron, *Mainstreaming*, supra note.
[144] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

genuine, much as is done in cases involving workers with asbestosis who suffer fear the likelihood of developing cancer.[145]

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 individuals' information for fraudulent purposes. As discussed in Part I, courts have found that if hackers obtain a plaintiff's personal data and uses 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 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.[146]

To return to a recent decision, in *Bradix v. Advance Stores Co., Inc.,* the court dismissed claims for lack of injury where plaintiff alleged that hackers obtained the defendant employees' names, Social Security Numbers, gross wages, and state where employees pay income taxes and used the information in unauthorized attempts to secure vehicle financing appearing on plaintiff's credit report because there was no proof that the attempts at fraud damaged plaintiff's credit score.[147] That hackers had personal data and attempted to use it makes clear that there is significant risk of future injury. Hackers—whose identities are unknown and 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' identity 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

[145] 538 U.S. 135, 1560-57 (2003) (analyzing federal Employers Liability Act).
[146] Daniel J. Solove and Paul Schwartz, The New PII Problem, NYU Law Review.
[147] 2016 WL 3617717 (E.D. La. July 6, 2016).

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 other similarly situated individuals have been victimized or have faced attempts to defraud 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, a fraudster has obtains a plaintiff's personal data, but nothing is known about its misuse. In those circumstances, the precise motive 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 motive. As a practical matter, the hackers' identities are unknown and thus such proof is illusive. Crucially, there is no need to require it. Hackers' criminal motive can be presumed. As the Seventh Circuit asked in *Remijas v. Neiman Marcus*, why else would hackers steal personal data if not for criminal purposes? 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 plaintiff's personal data. Nothing is known about the use of the data. The device might have been stolen for the device or for 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, among other things.

This case could go either way. If the data by itself or in combination with other data is not readily useable 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 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.[148]

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 upon 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 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 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?[149] 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.

[148] This scenario is quite common. State attorneys general have investigated cases involving the loss of backup tapes and laptops with personal data where it is unclear if the devices were simply misplaced or stolen. See Citron, *Privacy Policymaking*, *supra* note.

[149] 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, *Privacy Policymaking*, supra note.

8. Improper Access by an Organization's Employee

Suppose an employee improperly accesses records concerning 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 health data. This is a classic case 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 provide notice to people about data breaches, but they do little to redress any injuries caused. The cost of sending out breach notification letters can serve as a deterrent, but these laws are often strict liability and are not tied to blameworthy conduct. 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. 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 55 cases involving data security over the past 20 years. 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.

Private lawsuits serve 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."[150]

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 cumulatively as hundreds and perhaps thousands of organizations 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 wins.

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 it 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

[150] Storm, 90 F. Supp.3d at 368. Recognizing 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. Under both tests, context is an important consideration for the various factors. This in turn may make it difficult to obtain certification for classes involving thousands of people. Fed. R. Civ. P. 23(b)(3). 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 harms to overcome challenges to certification.

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 go undeterred. The consequences should be seen beyond the particular case. Data 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 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 up 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. Such an approach is not only dishonest, but also 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. Many of the reasons why data breach harms are not recognized as cognizable is because they push on many of the areas where the law is very gingerly developing. Some might argue that the law should turn away data harms until it is fully prepared to embrace them. That view, however, ignores the expressive function of the law.[151] 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 non-existent.

It is difficult to set aside the law's current difficulties when tackling the question of whether the law should recognize data 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 never grow or

[151] Danielle Keats Citron, *Law's Expressive Function in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009).

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 it functions fairly well, then one might be more accepting of it. The further away it is form 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 handling 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.[152] 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 to data breach harms. Various lines 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 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

[152] Citron, *Reservoirs*, *supra* note.

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 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 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.