NOTES

INTEGRATING INTEGRITY: CONFRONTING DATA HARMS IN THE ADMINISTRATIVE AGE

David J. Bier[*]

ABSTRACT

Each day brings with it a news report about how another company has suffered a data breach. But then what? Victims of data breaches have little or no recourse. Victims often struggle to overcome the constitutional standing requirement. When a legal settlement is reached, the actual compensation that victims receive is minimal. Businesses have weak incentives to strengthen security protocols, and there is no standard for what constitutes acceptable data protection practices.

This Note reconceptualizes data breaches, not as isolated events requiring specifically tailored remedies, but as societal harms that are sure to repeat themselves. Using past responses to other widespread risks, this Note outlines a modern solution to the problem of data breaches. By setting clear standards, re-aligning incentives for organizations that store data, and ensuring that impacted parties obtain meaningful recovery, the incidence of data breaches and their harmful effects can be minimized.

[*] J.D., Boston University School of Law, 2019; M.Ed., Secondary Education, Arizona State University, 2015; B.A., Government & International Politics and Conflict Analysis & Resolution, George Mason University, 2013. I would like to thank Professor Jay Wexler for his insight and guidance in drafting this Note and the editors and staff of the *Boston University Law Review* for their diligent work in preparing it for publication. More importantly, I would like to thank my family and friends for their encouragement and support throughout my academic career.

CONTENTS

INTRODUCTION

Data breaches are becoming increasingly common.[1] As more and more businesses, industries, and government bodies begin to rely upon data as an integral part of operations, data breaches will continue to plague consumers and businesses. In the aftermath of these intrusions into corporate and government infrastructure, however, the several parties to a data breach are left without many viable options to make themselves whole again. As two leading privacy law scholars have proclaimed, "[d]ata breaches have become an epic problem."[2]

Commonly, no post-breach remedy is available to harmed parties. And when one is available, it is woefully inadequate. The parties to a data breach, their relations to one another, the harms faced by each party, and the prevalence of international actors all contribute to the quandary. To better understand these issues, consider the recently reported breach of Equifax, one of the nation's three credit reporting agencies. The Equifax hack exposed the data of some 145.5 million U.S. customers.[3] The breach included individuals' names, Social Security numbers, dates of birth, addresses, and some individuals' driver's license numbers and credit card numbers.[4] Since between fourteen and thirty-three percent of data-breach victims ultimately become victims of fraud, at least twenty million Americans are likely to suffer real world consequences.[5] Initially, people were outraged that a large company like Equifax would "allow" their data to be compromised.[6] This criticism is not entirely without merit, as a subsequent investigation discovered that Equifax was alerted to a security vulnerability but did not take simple steps to secure its systems.[7]

---

[1] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 745 (2018) ("The number of people affected by data breaches continues to rise as companies collect more and more personal data in inadequately secured data reservoirs.").

[2] *Id.*

[3] *2017 Cybersecurity Incident & Important Consumer Information: Frequently Asked Questions*, EQUIFAX, https://www.equifaxsecurity2017.com/frequently-asked-questions [https://perma.cc/MQ9D-FVXN] (last visited Aug. 22, 2019) ("We identified a cybersecurity incident impacting approximately 145.5 million U.S. consumers.").

[4] *Id.*

[5] *See* ANNE JOHNSON & LYNETTE I. MILLETT, DATA BREACH AFTERMATH AND RECOVERY FOR INDIVIDUALS AND INSTITUTIONS: PROCEEDINGS OF A WORKSHOP 13 (2016) (summarizing speech by Beth Givens, Founder and Executive Director Emeritus of Privacy Rights Clearinghouse, offering statistics about percentages of breach victims that became fraud victims from 2011 to 2014).

[6] Elizabeth Warren (@SenWarren), TWITTER (Sept. 15, 2017, 12:08 PM), https://twitter.com/senwarren/status/908724324680523782?lang=en [https://perma.cc/UD8B-FQRE] ("Lot of people are outraged about the @Equifax data breach. I am too.").

[7] David Shepardson, *Equifax Failed to Patch Security Vulnerability in March*, REUTERS (Oct. 2, 2017, 10:52 AM), https://www.reuters.com/article/us-equifax-breach/equifax-failed-

Notwithstanding, Equifax was the victim of a criminal act whereby outside hackers infiltrated its corporate infrastructure to take something without permission. In fact, the hack may have been perpetrated by a state-sponsored intelligence service.[8] In addition to the public relations calamity, Equifax was subjected to congressional hearings,[9] regulatory action,[10] and litigation.[11]

Individuals whose data is hacked face substantial harm, but that harm is difficult for courts to conceptualize. Indeed, academics have devoted significant attention to finding ways for courts to better understand the future harms faced by data-breach victims.[12] For example, a victim of the Equifax breach who suffered only from the exposure of her credit card number can contact the issuing bank and receive a new number. At first glance, this may seem like a minor inconvenience at worst. But, in addition to the time costs imposed on the individual, it imposes a financial cost on the issuing bank (i.e., making the new card, mailing the new card, administrative costs, etc., multiplied by the tens of

to-patch-security-vulnerability-in-march-former-ceo-idUSKCN1C71VY [https://perma.cc/G2WA-M2VR] (noting Congressional testimony of former Equifax CEO that U.S. Homeland Security Department alerted Equifax of breach five months before hackers accessed consumer information).

[8] Michael Riley, Jordan Robertson & Anita Sharpe, *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG BUSINESSWEEK (Sept. 29, 2017, 9:09 AM), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros (describing facts suggesting state-sponsored actors perpetrated hack).

[9] *See An Examination of the Equifax Cybersecurity Breach: Hearing Before the S. Comm. on Banking, Hous., & Urban Affairs*, 115th Cong. 4-44 (2017) (testimony of Richard F. Smith, former Chief Executive Officer, Equifax); Joe Uchill, *House Panel Hits Equifax with Long List of Investigation Demands*, HILL (Nov. 17, 2017, 2:29 PM), http://thehill.com/policy/cybersecurity/360929-house-ec-hits-equifax-with-long-list-of-investigation-demands [https://perma.cc/8HNW-LKQR] (describing questions sent by House Energy and Commerce Committee to Equifax to supplement Congressional testimony of former Equifax CEO).

[10] Megan Gordon & Daniel Silver, *The Equifax Hack, SEC Data Breach, and Issuer Disclosure Obligations*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Oct. 5, 2017), https://corpgov.law.harvard.edu/2017/10/05/the-equifax-hack-sec-data-breach-and-issuer-disclosure-obligations/ [https://perma.cc/6VTH-2D8Z] (noting possibility of SEC enforcement actions when publicly traded companies fail to disclose cybersecurity intrusions).

[11] *See* Knepper v. Equifax Info. Servs., LLC, No. 2:17-cv-02368, 2017 WL 4369473, at *1 (D. Nev. Oct. 2, 2017) (noting that just four days after Equifax breach announcement, at least twenty-two cases had already been filed).

[12] *See, e.g.*, Solove & Citron, *supra* note 1, at 756 (arguing that data-breach harms derive from well-recognized common-law doctrines and should be sufficient to confer standing).

thousands of customers that may be impacted at any given bank).[13] A victim who lost control of immutable data, like her Social Security number or date of birth, will now incur pecuniary costs to pay for credit monitoring services, spend valuable time scouring financial statements for suspicious charges, and may even develop anxiety over the possibility of future identity theft.[14]

At present, secondary victims, like the issuing bank in the above example, have no means of recuperating these losses, and individuals seeking legal redress are often stymied by the judicial doctrine of standing. Standing, derived from Article III of the U.S. Constitution, confers federal court jurisdiction only when there is a "case" or "controversy."[15] In the landmark case *Lujan v. Defenders of Wildlife*,[16] the court laid out the three prongs of the standing inquiry: in order for a plaintiff to have standing, she must show (1) an injury-in-fact, (2) that is fairly traceable to the defendant, and (3) which is susceptible to redress by a favorable judicial decision.[17] Data-breach victims seeking to become plaintiffs in suits against breached organizations, which can be either public or private entities,[18] are often turned away at the first stage of the standing inquiry for failure to identify a concrete and particularized "injury in fact."[19]

However, given the intangible and long-lasting features of the harms faced by data-breach victims, even a "successful" outcome may prove to be inadequate in the near future. For example, after health insurance provider Anthem suffered a breach, it settled with the plaintiff class for 115 million dollars.[20] At first blush, this sounds like a resounding victory for customers. But after the plaintiffs'

[13] Justin C. Pierce, Note, *Shifting Data Breach Liability: A Congressional Approach*, 57 WM. & MARY L. REV. 975, 982-85 (2016) (describing harms to merchants and issuing banks when retailer like Target suffers data breach).

[14] Solove & Citron, *supra* note 1, at 774-78 (outlining approach for judiciary to assess future risk and anxiety experienced by data-breach victims).

[15] U.S. CONST. art. III, § 2.

[16] 504 U.S. 555 (1992).

[17] *Id.* at 560-61.

[18] *See* U.S. JUDICIAL PANEL ON MULTIDISTRICT LITIG., MDL STATISTICS REPORT—DOCKET TYPE SUMMARY 3 (Nov. 15, 2017), http://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_Type-November-15-2017.pdf [https://perma.cc/LYE2-Y85P] (listing pending litigation against private entities like Yahoo! and public entities like U.S. Office of Personnel Management arising from data breaches).

[19] Solove & Citron, *supra* note 1, at 739 ("The majority of the cases, however, have not turned on whether the defendants were at fault. Instead, the cases have been bogged down with the issue of harm. No matter how derelict defendants might be with regard to security, no matter how much warning defendants have about prior hacks and breaches, if plaintiffs cannot show harm, they cannot succeed in their lawsuits.").

[20] Settlement Agreement and Release at 14, *In re* Anthem, Inc. Data Breach Litig., No. 5:15-md-02617 (N.D. Cal. June 23, 2017), ECF No. 869-8 ("Defendants agree to make a settlement payment of one hundred and fifteen million United States Dollars . . . .").

lawyers collected thirty million dollars in fees,[21] the remaining money was enough to pay each plaintiff approximately fifty dollars in cash, or about two years of credit monitoring.[22] Additionally, the familiar doctrine of claim preclusion will bar those plaintiffs from seeking further redress. But what happens when the information from that hack is used to steal the individual's identity three years later, when the plaintiff is no longer afforded the benefit of free credit monitoring? The harm sustained from the breach is still the proximate cause of the new injury, and the individual is left with several serious problems[23] and no prospect of further recovery.

While individuals need a more complete remedy, individual harms are merely one part of a complex situation. To adequately protect the interests of the several parties impacted by a data breach, prevent future data breaches, and improve the governmental response, a new approach is needed. Data breaches, taken together, should be thought of as an inevitable public harm, rather than isolated and discrete incidents. This broadened perspective is more helpful for policy creation and leads to a better solution.

The Delineated Approach Toward Addressing Data Breaches ("DATA-DB") is a comprehensive approach to reducing the incidence of data harms by modifying incentives to ensure that entities are adequately protecting stored data. Through the imposition of small taxes on certain data collection practices and data transfers between entities, less data will be collected and stored data will be transferred less frequently, reducing that data's exposure to future breaches. DATA-DB also incorporates the Data Harm Adjudication Board ("DHAB"), which will serve as a forum to remedy data harms impacting the wide variety of parties that may be affected by a given breach.

This Note proceeds in three parts. Part I sets out the current landscape of data breaches and the resulting litigation. Part II then provides a brief overview of government responses to historical instances where the public was faced with the risk of serious harm. Lastly, Part III sketches the outlines of DATA-DB to better resolve this novel, complex, and ballooning societal harm.

---

[21] *Id.* at 26 ("Defendants agree not to oppose a request for an award of attorneys' fees and costs that does not exceed 33% of the Settlement Fund ($37,950,000) in attorneys' fees . . . .").

[22] Ryan Black, *Should the US Adopt a Data Breach Safety Net?*, INSIDE DIGITAL HEALTH (Oct. 27, 2017), http://www.hcanews.com/news/should-the-us-adopt-a-data-breach-safety-net [https://perma.cc/9TUP-GZW5].

[23] *Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Subcomm. on Tech., Terrorism, & Gov't Info. of the S. Comm. on the Judiciary*, 106th Cong. 30-38 (2000) (statement of Beth Givens, Director, Privacy Rights Clearing House) (outlining problems faced by identity theft victims).

I. DATA-BREACH LANDSCAPE

The International Organization for Standardization defines "data breach" as a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed."[24] While the term "data breach" may also include physical objects, like paper records,[25] this Note focuses on a more contemporary concern—the dramatic and disturbing increase in breaches of digital records.

Data breaches today are commonplace, attracting front-page attention from the business section of newspapers across the country.[26] The proliferation of data breaches has been dramatic; as of this Note's publication, there have been at least 9046 *reported* data breaches since 2005, in addition to the countless others that were either not detected or detected but not reported.[27] These breaches have impacted organizations from large public companies[28] to government agencies at both the state[29] and federal levels,[30] and in 2019, breaches may cost organizations around the world upwards of two trillion dollars.[31] Not only can data breaches impact organizations of all stripes, but each breach can impact millions of individuals.[32] As private organizations and governmental bodies around the world continue the shift towards "data economies"[33] that rely heavily

[24] JOINT TECH. COMM., INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMM'N, ISO/IEC 27040: INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—STORAGE SECURITY § 3.7 (2015), https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en [https://perma.cc/Q75E-QT8R] (providing guidelines for security of data storage).

[25] Some of the most infamous events in U.S. history indeed qualify as data breaches. The Watergate scandal, for example, began with an old-fashioned "data breach."

[26] *See, e.g.*, Mike Isaac, Katie Benner & Sheera Frenkel, *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES, Nov. 21, 2017, at B1.

[27] *Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breaches [https://perma.cc/5FAU-WPV3] (last visited Aug. 22, 2019) (providing live-updated number of data breaches made public since 2005).

[28] Petition for Writ of Certiorari at 2, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (No. 11-1128), 2012 WL 865211, at *2 (listing hacks involving Sony and Zappos among others).

[29] *Id.* at *2 (including Texas Comptroller's Office).

[30] *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1, 8 (D.D.C. 2017), *aff'd in part, rev'd in part*, 928 F.3d 42 (2019).

[31] *Data Breach Costs Will Soar to $2T: Juniper*, CREDIT UNION NAT'L ASS'N: NEWS (May 15, 2015), https://news.cuna.org/articles/105948-data-breach-costs-will-soar-to-2t-juniper [https://perma.cc/9RF3-BLBV] (describing 2015 report's finding that "[i]n less than five years, the annual cost of data breaches at the global level will skyrocket to $2.1 trillion").

[32] *See, e.g.*, Petition for Writ of Certiorari, *supra* note 28, at *2 (noting tens of millions impacted by just small handful of breaches).

[33] *Data is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

on individuals' personal data, the number of people impacted by data breaches will continue to rise due to organizations' collection of "more and more personal data in inadequately secured data reservoirs."[34] Thus, it is safe to say that data breaches, and the resulting litigation, are here to stay.[35]

Several features of modern data breaches result in peculiar harms that courts have been loath to recognize.[36] These features also have created seemingly intractable policy issues that are matters of legislative concern unfit for judicial resolution. This has resulted in a series of contentious court decisions revolving around the harm aspect of standing under Article III of the U.S. Constitution. In order to devise a program to better remedy the harms appurtenant to data breaches, it is imperative to understand the scope and impact of the data breaches, the factors that combine to make data breaches unique within our legal system, and the way that litigation over data breaches is currently being handled. This Part examines each of these matters in turn.

("Although signs of the data economy are everywhere, its shape is only now becoming clear.").

[34] Solove & Citron, *supra* note 1, at 745 (stating increasing need for attending to harms caused by data breaches).

[35] The mushrooming of data-breach litigation was predicted as early as 2006. *See* Don A. Smith, *The Still Growing Problems of Data Breach and Identity Theft*, 123 BANKING L.J. 919, 924 (2006) ("[I]t seems likely that courts will experience an increasing number of claims related to data breach and identity theft."). This prediction has borne out in the number of suits over data breaches that have been consolidated as multidistrict litigations ("MDL"). *See* U.S. JUDICIAL PANEL ON MULTIDISTRICT LITIG., *supra* note 18, at 3 (listing active litigation related to twelve separate data breaches). Data-breach claims are particularly well-suited for MDL consolidation. The U.S. Code provides that "[w]hen civil actions involving one or more common questions of fact are pending in different districts, such actions may be transferred to any district for coordinated or consolidated pretrial proceedings." 28 U.S.C. § 1407(a) (2012). One can easily imagine how a single data breach that impacts, say, ten million users, would fall under this statutory provision. After a few dozen of those ten million users, spread across the country, file claims in federal court concerning a common nucleus of operative facts, it promotes the "just and efficient" resolution of those claims to allow one judge to handle the pretrial proceedings. *Id.* (providing that transfer shall be made upon "determination that transfers for [consolidated pretrial] proceedings will be for the convenience of parties and witnesses and will promote the just and efficient conduct of such actions"); *see, e.g.*, Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 630 n.68 (2018) (noting that, as of January 11, 2018, at least seventy-six civil actions arising from Equifax breach had been consolidated); Aaron Blumenthal & Andre M. Mura, *In the Breach*, TRIAL, Sept. 2017, at 30, 32 ("Many large data breaches result in cases being filed all over the country, which may lead to consolidation in a single federal district court for multidistrict litigation."). Thus, it seems the pending MDL docket is a useful tool to monitor ongoing data breach litigation in federal court.

[36] *See infra* Section I.A.

A. *Unique Features of Data-Breach Harms*

The proliferation of data breaches has important implications when considering how subsequent litigation over breach-inflicted harms should be addressed. Each of these features may not, on its own, be entirely unique. Said another way, each feature of a data breach, by itself, arguably has analogues in other areas of the law. Yet, the combination of all of the features make data breaches unique in our legal system, providing a plausible explanation as to why judicial resolution has disappointed many aggrieved plaintiffs.[37]

1. Intangible, Long-Term Harms

Perhaps the most significant practical impediment to data-breach victims recovering in court is the intangible, long-term nature of the harms they often face. To be sure, some of the harms are tangible, like fraudulent credit card charges (stolen payment card information) or fraudulent attempts to open new credit cards or bank accounts (stolen Social Security number).[38] Yet, most individual harms involve the risk of future injury, losses incurred in protecting oneself against those future injuries, and emotional distress or anxiety over what an ill-intentioned data thief will do with one's data in the future.[39] To varying degrees, these harm theories have not proven very successful for plaintiffs, no matter how legitimate they may be.

Plaintiffs' lack of success may be due in large part to the intangible nature of these harms. Courts have, for example, dismissed risk-of-future-harm injuries as

---

[37] Additionally, there are a number of issues incident to data breaches that are beyond the scope of this Note. For example, data breaches may carry national security implications. Special Counsel Robert Mueller led an investigation into Russia's interference with the 2016 U.S. elections. As part of that investigation, a grand jury issued an indictment against numerous Russian nationals and Russian business entities for a litany of criminal behaviors. *See* Indictment, United States v. Internet Research Agency, No. 1:18-cr-00032 (D.D.C. Feb. 16, 2018). Among the charges are five counts of "Aggravated Identity Theft" based on the use of "the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent." *Id.* ¶ 41; *see also* Clare Sullivan, *The 2014 Sony Hack and the Role of International Law*, 8 J. NAT'L SECURITY L. & POL'Y 437, 441 (2016) (quoting former White House Press Secretary Josh Earnest in briefing describing 2014 hack of Sony stating "this is something that's being treated as a serious national security issue"). These national security matters may also implicate the military, similarly committed to exclusive control of the federal government. *See* Ellen Nakashima, *U.S. Strike on Election Day Targeted Russian Trolls*, WASH. POST, Feb. 27, 2019, at A1 (noting military response to cyber-threat to election security).

[38] *See* Plaintiffs' Consolidated Opposition to Defendants' Motions to Dismiss at 7-22, *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1 (D.D.C. 2017) (No. 15-1394) (describing plaintiffs' actual economic injuries), *aff'd in part, rev'd in part*, 928 F.3d 42 (2019). Of course, this must be taken with a grain of salt considering the source's persuasive purpose and framing.

[39] *See* Solove & Citron, *supra* note 1, at 750-54.

too speculative, sometimes even in the face of allegations that plaintiffs' information was taken in a malicious theft,[40] as opposed to an accidental misplacement of a data storage device.[41] The malicious digital hack or physical theft of a device seems to import a higher degree of nefarious intent, yet courts do not generally recognize this as a sufficient indicator of the future harms that plaintiffs fear.[42]

Given, however, that from 2011-2014, somewhere between fourteen percent and thirty-three percent of data-breach victims ultimately became victims of fraud,[43] some individuals take matters into their own hands. Victims of data breaches will, for example, make out-of-pocket expenditures to purchase credit monitoring services or place freezes on their credit reports.[44] When plaintiffs spend money to protect themselves against these future injuries, statistically certain to impact a given number of data-breach victims, courts are dismissive of the plaintiffs' apparent "attempts to 'manufacture' injury."[45] Lastly,

[40] *See* Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1019-21 (D. Minn. 2006) (distinguishing between present injury and "anticipation of future injury that has not materialized"); Solove & Citron, *supra* note 1, at 750 ("[I]ncreased risk of identity theft is regarded as too speculative . . . .").

[41] *See* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (finding "enhanced risk of future identity theft too speculative" where plaintiffs "uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identify theft, nor . . . that the thief stole the laptop with the intent to steal their private information").

[42] *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 766, 771-72 (8th Cir. 2017) (holding that, despite hackers' use of "malicious" software, plaintiffs' "complaint has not sufficiently alleged a substantial risk of identity theft, and plaintiffs' allegations of future injury do not support standing in this case"). *But see, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

[43] JOHNSON & MILLETT, *supra* note 5, at 13 ("Givens offered some statistics about fraud: In 2011, one in five breach victims became a fraud victim. In 2012, this proportion rose to one in four, and in 2013, it was one in three. In 2014, this proportion decreased to one in seven, mostly thanks to the remediation efforts stemming from the large point-of-sale data breaches at Target and Home Depot (figures from research provided by Javelin Strategy and Research), Givens said. To rectify those breaches, credit card companies issued cardholders new cards, which was expensive but effective at reducing fraud, as the numbers show.").

[44] Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N: CONSUMER INFO. BLOG (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/S9RX-8LXW] (recommending "steps to take to help protect yourself after a data breach").

[45] *See* Solove & Citron, *supra* note 1, at 753 (first citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013); then citing Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 470-71 (D.N.J. 2013)).

plaintiffs' complaints frequently allege anxiety as an additional harm,[46] but this theory is perhaps the least successful of the three—a strong statement given the ineffectiveness of the other two approaches.[47]

The issue of demonstrating harm is further complicated in the data-breach context by the long-term nature of the harm. Because the law does not yet recognize the mere breach of personally identifiable information ("PII") as constituting a legal injury, despite persuasive research that such an injury ought to be recognized,[48] individuals often must wait until they are able to show a subsequent negative event—a vested harm.[49] Such a vested harm may not occur for years, especially in cases where the breached information is immutable, like a Social Security number or date of birth.[50] This delay, while making the harm from data breaches worse, is ironically a critical factor that hinders plaintiffs' ability to get a claim into court.

2. Unbound Individual Risk

Data breaches also present a risk to nearly everyone participating in modern society. The digital nature of data breaches transcends many of the limitations impacting other types of large-scale litigation. For example, consider a seemingly analogous claim: toxic exposure torts.[51] In analyzing this comparison, the Third Circuit found a difference between data breaches and toxic-exposure claims, noting that "exposure to a toxic substance causes injury; cells are damaged and a disease mechanism has been introduced."[52] By contrast, the

[46] *See id.* at 753-54 (describing plaintiffs' argument that "data breaches caused them emotional distress (in particular, anxiety)").

[47] *See id.* at 753 (noting "courts have rejected [anxiety] claims nearly every time").

[48] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2012) (arguing for recognition of subjective privacy harms, such as "unease caused by a massive data breach").

[49] *See* Solove & Citron, *supra* note 1, at 754 ("[Courts] require harms to be vested—already materialized in the here and now.").

[50] *Id.* at 757 ("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." (omission in original) (quoting Andrea Peterson, *Data Exposed in Breaches Can Follow People Forever. The Protections Offered in Their Wake Don't.*, WASH. POST: THE SWITCH (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/))); *id.* at 758 ("Social Security [n]umbers have a very long shelf life—a bad guy that's smart won't use it immediately, he'll keep a hoard of numbers and use them in a couple of years." (alteration in original) (quoting Peterson, *supra*)).

[51] *See* Clara Kim, Note, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 570 (2016) (noting cases in which court analogized to toxic exposure tort claims).

[52] Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011).

harms from data breaches were found to be less certain.[53] Another potentially analogous claim the court considered was a products-liability situation arising from an implanted medical device. And while the court claimed that those cases have a "quantifiable risk of failure," the court went on to assert that data breaches without alleged misuse present "no change in the status quo."[54]

There is, however, a notable difference between data breaches and these somewhat analogous situations—one that makes data breaches far more troubling as a societal harm and, as a result, makes the need for just resolution that much greater. These situations implicate some widespread harm that impacts only discrete populations (those living near the toxic substance release or those who received the defective medical device) in a single event or occurrence. Conversely, data breaches have the potential to reach nearly everyone participating in modern society, and to reach individuals multiple times, possibly exposing different types of information. While any single breach can arguably reach a similarly discrete, albeit exponentially larger group of individuals, data breaches can transcend the physical realities of other harms to impact more people more frequently. And while the privacy- and risk-based harms incurred from data loss are arguably less serious than physical, risk-based maladies resulting from exposure to a toxic substance or the implant of a defective medical device, it is clear that the law should be capable of remedying both types of harm.

3. Multiple Classes of Parties

Furthermore, data breaches are unique in the number of different parties they impact and the relations between those parties. It is valuable here to consider the different classes of parties that have and will continue to fall victim to data breaches, for each class bears a unique relationship to the others. Perhaps most obviously, the first class is individuals whose data has been compromised. The lion's share of data-breach litigation features a party from this class as the plaintiff, and the predominant thrust of academic research focuses on the harms this group faces along with the subsequent litigation.[55] Given computer systems' ability to maintain records of huge numbers of individuals, this party commonly includes millions of people.[56]

The second class of parties is the breached entities. In any given breach, whether it targets a private company or a governmental organization, the breached entity incurs a slew of post-breach costs. Certain types of entities commonly fall within this class. Health-related firms (including patient care

[53] *See* Kim, *supra* note 51, at 571 n.127 ("[T]he court seemed to put greater weight on the predictability of health consequences than harmful consequences from data breaches . . . .").

[54] *Reilly*, 664 F.3d at 45.

[55] *See, e.g.*, Solove & Citron, *supra* note 1, at 738-39 (discussing harms suffered by clients of company that failed to protect customer data).

[56] *See, e.g.*, Petition for Writ of Certiorari, *supra* note 28, at 2.

providers, insurers, etc.) are frequent breach targets.[57] These breaches are problematic because, on top of sensitive health data, health-care companies often retain a trio of PII particularly useful to malicious actors—an individual's full name, date of birth, and Social Security number—along with financial information. Web service companies can be attractive because they retain user data on hundreds of millions of users. In addition to usernames and passwords, these breaches can include dates of birth along with security questions and answers.[58] Many breaches target a specific subclass of web service companies—retailers—in search of individuals' financial data.[59] These breaches necessarily implicate, as a third class of parties, financial service providers like banks and credit unions.

In addition to retaining counsel to assist with certain impending litigation, potential congressional hearings,[60] and potential regulatory action,[61] a breach target must hire a data-forensics firm to ensure that all backdoors have been closed so the hacker is no longer able to access the target's computer systems.[62] This can be a complicated, multistep process.[63] These impacts alone are significant, and give no mention to the reputation and goodwill harms inflicted on the breached merchant. In the Target breach, for example, the company

[57] *See, e.g.*, Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits over Data Breach*, REUTERS (June 23, 2017, 6:19 PM), https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML [https://perma.cc/YK58-KAPJ].

[58] *See, e.g.*, Laura Hautala, *Alleged LinkedIn Hacker Extradited from Czech Republic to US*, CNET (Mar. 30, 2018, 3:41 PM), https://www.cnet.com/news/alleged-linkedin-dropbox-hacker-yevgeniy-nikulin-extradited-to-us/ [https://perma.cc/AKE4-5CET] (LinkedIn 2012 breach); Alfred Ng & Laura Hautala, *Yahoo Hit in Worst Hack Ever, 500 Million Accounts Swiped*, CNET (Sept. 22, 2016, 4:42 PM), https://www.cnet.com/news/yahoo-500-million-accounts-hacked-data-breach/ [https://perma.cc/PR66-82EY] (Yahoo 2014 breach, which compromised email addresses, passwords, and birth dates).

[59] *See, e.g.*, Jennie Bell, *Court Reopens 2012 Zappos Data Breach Litigation*, FOOTWEAR NEWS (Mar. 9, 2018, 3:25 PM), http://footwearnews.com/2018/business/retail/zappos-appeals-court-lawsuit-data-breach-identity-theft-517197/ [https://perma.cc/R3UU-EGDJ] (Zappos 2012 payment system breach); Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers*, USA TODAY (May 23, 2017, 6:42 PM), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/ [https://perma.cc/YJ6C-JWS5] (Target 2013 payment system breach).

[60] *See, e.g.*, *supra* note 9 (describing congressional hearings related to Equifax breach).

[61] *See, e.g.*, *supra* note 10 (describing potential regulatory actions related to Equifax breach).

[62] *See* INFO. SYS. AUDIT & CONTROL ASS'N, OVERVIEW OF DIGITAL FORENSICS 4 (2015) ("When a breach occurs, the forensic analyst must locate the point of compromise.").

[63] *Id.* at 7 (providing overview of digital forensics scientific process).

offered ten percent off in-store sales in an effort to entice customers to return to the store during the critical holiday period.[64]

Beyond these two "primary" parties to a data breach, a data breach may also impact a series of "secondary" parties. For example, when a retailer is hacked in an effort to obtain individuals' financial data, a host of banks incur costs.[65] And while one may feel little sympathy for large national banks that can easily absorb associated costs, post-breach actions may result in costs that present significant hardships for small banks and credit unions.[66] Costs to a financial service provider may include creating and mailing replacement cards, monitoring customer accounts for fraudulent transactions, and in many instances, covering the costs of those fraudulent transactions.[67]

Yet another party, collectively comprising another class, is largely ignored in litigation. Most breaches include a hacker that perpetrated the data breach.[68] A number of the most serious hacks are attributed to state-sponsored groups, from military units to intelligence services.[69] Yet, courts do not and likely will not develop a way of holding these parties accountable. Beyond the international law issues that abound in such a situation[70] and the limits of federal court jurisdiction, actually enforcing a judgment against such an actor is virtually certain to be futile.

---

[64] Sara Germano, *Target's Data-Breach Timeline*, WALL STREET J.: CORP. INTELL. (Dec. 27, 2013, 6:28 PM), https://blogs.wsj.com/corporate-intelligence/2013/12/27/targets-data-breach-timeline (providing timeline related to Target's data breach and ensuing investigation).

[65] *See* Pierce, *supra* note 13, at 981 (discussing banks involved in typical retail transaction).

[66] *See id.* at 984 (noting disproportionate impact on small banks).

[67] *See id.* (noting costs of, for example, mailing new cards and monitoring customer accounts for fraudulent transactions).

[68] The law has long been equipped to address physical data breaches, such as a claim against one who steals a physical data storage device or a claim against an employee whose negligent failure to follow company practice regarding a data storage device resulted in a loss. This paragraph instead focuses on the often anonymous and/or state-sponsored activity behind electronic data breaches.

[69] *See* 1 ROBERT S. MUELLER III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 36 (2019) ("Two military units of the GRU carried out the computer intrusions into the Clinton Campaign, DNC, and DCCC: Military Units 26165 and 74455."); *id.* at 1 ("Second, a Russian intelligence service conducted computer-intrusion operations against entities, employees, and volunteers working on the Clinton Campaign and then released stolen documents.").

[70] *See generally* Peter Margulies, *Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy*, 24 IND. J. GLOBAL LEGAL STUD. 459 (2017) (describing several international law responses Obama administration deployed to address data privacy in wake of Snowden leaks); David E. Sanger & William J. Broad, *Pentagon Plan Would Expand Nuclear Policy*, N.Y. TIMES, Jan. 17, 2018, at A1.

B. *Illustration of the Issues: The Equifax Breach*

On September 7, 2017, Equifax announced that its computer systems had been breached by malicious hackers, compromising private data of over 145.5 million Americans.[71] This breach illustrates intangible harms, unbound individual risks, and the multiple classes of parties involved perhaps better than any other. It also illustrates the remarkably narrow approach that lawmakers have taken thus far in response to data-security incidents. Above all, it demonstrates the dire need for a new system to handle data-breach litigation and ensure an appropriate, adequate remedy for all.

First, from the individual victims' perspective, the hack brought about the long-term, intangible harms characteristic of a data breach. The hack exposed individuals' "names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."[72] Since immutable data was among that taken in the breach, those affected have felt the impacts long after the breach.[73] Despite the fact that over two years have passed since the breach, it remains unclear how many will face financial loss. And as opposed to a breach that impacts a particular retailer or online service, this hack demonstrates the unlimited individual exposure hallmark of digital attacks. After all, this breach impacted nearly half of the U.S. population.[74]

Since Equifax is a credit reporting agency, it is very different from other hacks where, for example, a customer could purportedly be afforded an opportunity to read the company's privacy policy before deciding whether or not she would create an account and submit her PII. Instead, Equifax maintains records from individuals who have engaged with the modern economy in other ways—taking out a car loan or applying for a credit card, for example.[75] The unlimited individual risk associated with data breaches is shown through the sheer scale of the breach and the nature of a credit reporting agency's role in the U.S. economy, which can lead to massive ramifications that are felt for many years to come.

---

[71] *Equifax Data Breach Affected Millions More than First Thought*, CBS NEWS (Oct. 2, 2017, 5:55 PM), https://www.cbsnews.com/news/equifax-data-breach-millions-more-affected [https://perma.cc/7NVQ-V9VD] (stating that estimated 145.5 million Americans were impacted); Alyssa Newcomb, *Massive Equifax Data Breach Could Affect Half of the U.S. Population*, NBC NEWS (Sept. 7, 2017, 7:27 PM), https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686 [https://perma.cc/3LFR-28TD] (discussing Equifax's announcement of breach).

[72] Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N: CONSUMER INFO. BLOG (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/A7T5-7GD4].

[73] *See* Anna Werner, *Months After Massive Equifax Data Breach, Victims Struggling to Recover*, CBS NEWS (Jan. 9, 2018, 6:41 PM), https://www.cbsnews.com/news/equifax-data-breach-victims-struggling-to-recover [https://perma.cc/JLW6-RHW2] (explaining how "victims have struggled to regain their identities and clean up their credit reports").

[74] Newcomb, *supra* note 71.

[75] *See id.*

The breach also shows how multiple classes of parties are impacted—for each individual impacted by actual fraudulent charges, financial institutions must begin the process of reissuing cards and covering the cost of these charges.[76]

The breach also exhibited several of the hallmarks of modern data breaches that have drawn legislators' ire at the state and federal levels. Equifax did not notify the public until six weeks after the breach occurred.[77] Some forty-eight states have laws mandating disclosure and notification to impacted individuals whenever a data breach occurs.[78] While there is no federal law mandating disclosure, it has been a key element in several proposed bills.[79] Senators Elizabeth Warren and Mark Warner proposed the Data Breach Prevention and Compensation Act of 2018 to address issues demonstrated by the Equifax breach, such as patterns of security failures.[80] Yet, this bill is remarkably narrow in scope, only addressing data security at credit reporting agencies ("CRAs").[81] While CRAs are undoubtedly attractive targets for hackers, as the Equifax breach illustrates, they make up a relatively miniscule slice of the organizations, both governmental and nongovernmental, that store individuals' PII. The problem of data breaches is far larger than the Equifax hack, and the threat is much greater than the Senators' proposed legislation would address.

C. *Standing Issues: Harm Today, Causation Tomorrow*

Standing has presented a significant obstacle for plaintiffs seeking to redress data-breach injuries. In order to confer standing, the injury to the plaintiff must

---

[76] *See* Werner, *supra* note 73 (describing how one victim "got a bill for a hotel stay in Las Vegas" despite not visiting the city, not to mention some fifteen fraudulent accounts opened in her name).

[77] *See* Newcomb, *supra* note 71 (stating that breach was discovered on July 29, 2017); Press Release, Equifax, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 [https://perma.cc/7MWQ-NF4C].

[78] *See generally* BAKERHOSTETLER, STATE DATA BREACH LAW SUMMARY (2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf [https://perma.cc/HP7C-XBNL].

[79] *See, e.g.*, Data Breach Prevention and Compensation Act of 2018, S. 2289, 115th Cong. § 4 (2018) (legislation proposed by Sens. Warner & Warren); Data Security and Breach Notification Act, S. 2179, 115th Cong. § 3 (2017) (legislation proposed by Sens. Nelson, Blumenthal & Baldwin).

[80] *Data Breach Prevention and Compensation Act Fact Sheet*, ELIZABETH WARREN: NEWSROOM (Jan. 10, 2018), https://www.warren.senate.gov/files/documents/Data%20Breach%20Prevention%20and%20Compensation%20Act%20One-Pager.pdf [https://perma.cc/EXB4-9JDG] (explaining how proposed act addresses problems demonstrated by Equifax breach).

[81] *See id.* (stating that Act gives "Federal Trade Commission more direct supervisory authority over data security at CRAs").

be "concrete and particularized"[82] and "actual or imminent, not 'conjectural' or 'hypothetical.'"[83] Yet, an injury that is "certainly impending" may be sufficient.[84] This language, strictly construed, seems to foreclose standing when an injury has not yet occurred because it seems to lack concreteness or, in the alternative, because it is not guaranteed to happen. Yet, the Court has made clear that these strict interpretations are not correct. In *Clapper v. Amnesty International USA*,[85] the Court elaborated on the term "certainly impending" and noted that it should not be interpreted so literally.[86] Instead, a "substantial risk" of future harm may be sufficient.[87] Several years later, in *Spokeo, Inc. v. Robins*,[88] the Court addressed the relationship between the "substantial risk" theory and the concreteness requirement, stating that "the risk of real harm [can] satisfy that requirement."[89]

Despite these developments, the Circuits remain split on whether data-breach harms constitute a cognizable "injury in fact" under a "risk of future injury" theory.[90] The Third, Sixth, and D.C. Circuits have all stated that the risk of future injury resulting from a data breach is an injury sufficient to confer standing.[91] The Seventh and Ninth Circuits agree with this position, but the Ninth Circuit

[82] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

[83] *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

[84] *Whitmore*, 495 U.S. at 158 (explaining that "[a]llegations of possible future injury do not satisfy the requirements" but an injury that is "certainly impending" can "constitute injury in fact").

[85] 568 U.S. 398 (2013).

[86] *Id.* at 414 n.5 ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about.").

[87] *Id.* ("In some instances, we have found standing based on a 'substantial risk' that the harm will occur . . . .").

[88] 136 S. Ct. 1540 (2016).

[89] *See id.* at 1543.

[90] *See* Solove & Citron, *supra* note 1, at 750-52 (explaining that courts reject increased risk of future identity theft or fraud as theory of harm); *supra* Section I.A.1 (discussing how courts have rejected increased risk of harm as too speculative); *see generally* Kim, *supra* note 51, at 570 (discussing increased risk of harm as a hypothetical injury that does not establish standing).

[91] *See* Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (finding "substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 640 (3d Cir. 2017) (finding concrete injury based on dissemination of private information in violation of Fair Credit Reporting Act); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (finding substantial risk of harm "[w]here a data breach targets personal information").

issued its opinion before *Clapper* and *Spokeo*,[92] and the Seventh Circuit issued its opinions after *Clapper* but prior to *Spokeo*.[93] Conversely, the First, Fourth, and Eighth Circuits have held that data breaches do not generate "risk of future injury" sufficient to confer standing.[94] This split has spurred a number of law review articles and notes that, for the most part, urge courts to find that data-breach plaintiffs' harms present a "substantial risk" sufficient to confer standing.[95]

Although courts are currently struggling primarily with the "actual injury" aspect of standing, it seems that the onslaught of massive data breaches will soon give rise to a different defense—causation. Recall that *Lujan* requires that an injury be "fairly . . . trace[able] to the challenged action of the defendant."[96] Consider that the Equifax hack, which included individuals' immutable PII like Social Security numbers, reached 145 million people.[97] That is well over one-

[92] *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding plaintiffs alleged "credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" sufficient to constitute injury-in-fact).

[93] *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (finding concrete injury where plaintiffs alleged "increased risk of fraudulent charges and identity theft"); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (finding that because purpose of hack is presumably to make fraudulent charges or steal identities, it is plausible to infer substantial risk of harm from data breach).

[94] *See In re* SuperValu, Inc., 870 F.3d 763, 771 (8th Cir. 2017) (holding that mere possibility of future harm is insufficient for standing); Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (finding that mere theft, without more, is insufficient to constitute substantial risk of harm); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (finding that because plaintiff "does not identify any incident in which her data has ever been accessed by an unauthorized person, she cannot satisfy Article III's requirement of actual or impending injury").

[95] *See, e.g.*, Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1332 (2017) (arguing that "traditional limitations on privacy doctrines should be revised in an online era where personal data is readily accessible to unwanted third parties, including hackers or the government"); Solove & Citron, *supra* note 1, at 737 (arguing that "courts are far too dismissive of certain forms of data-breach harm and can and should find cognizable harms"); Kim, *supra* note 51, at 545 (arguing for adoption of Seventh Circuit's approach and "[l]essening the burden of standing requirements for consumer plaintiffs in data breach cases"); Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 80 (2017) (arguing that "Congress should pass a comprehensive data breach statute that would confer standing upon victims of data breach").

[96] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (alterations in original) (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976)).

[97] *See Equifax Data Breach Affected Millions More than First Thought*, *supra* note 71.

third of the U.S. population, which is approximately 329 million.[98] While not guaranteed, it is a near statistical certainty that at least some of those individuals also had their immutable PII breached in at least one other incident. A few breaches that reached immutable PII (including, for example, Social Security numbers, names, and addresses) include: Anthem (seventy-nine million subscriber records);[99] Uber (fifty-seven million customer records and six hundred thousand driver records);[100] and JPMorgan Chase (seventy-six million individual records and seven million small business records).[101]

A brief anecdote may elucidate this issue.[102] Let's assume that an individual, Victim Vince, had his name, Social Security number, address, and date of birth accessed in each of the following verified data breaches: Equifax (May-July 2017), Anthem (February 2015), and JPMorgan Chase (June-July 2014). In August of 2017, Fraudster Frank successfully opens bank accounts, takes out personal loans, and applies for a new credit card by fraudulently using Vince's PII. With clear injury, Vince seeks to sue Equifax in federal court. While Equifax may have been the hack temporally closest to the fraudulent activity, there is more than a mere possibility that Frank obtained Vince's PII by buying it directly from the hacker who breached JPMorgan Chase's system. After obtaining it from the hacker, Frank held onto the data for a few years, knowing it was extremely unlikely that Vince would change his Social Security number and that it is entirely impossible for him to change his date of birth. Of course, neither Vince nor Equifax's attorneys know that Frank is lying in wait, holding onto the data and waiting to deploy it. It is impossible for either party to discover this information. After a brief round of discovery confined to the issue of standing,[103] however, Equifax's legal team discovers that Vince received notice

[98] CIA, *United States*, WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/print_us.html [https://perma.cc/3PD7-4HCS] (last visited Aug. 22, 2019).

[99] *See* Pierson, *supra* note 57 (stating that about seventy-nine million people's personal information was compromised).

[100] Dave Lee, *Uber Concealed Huge Data Breach*, BBC NEWS (Nov. 22, 2017), https://www.bbc.co.uk/news/amp/technology-42075306 [https://perma.cc/V6P5-CUU3].

[101] *See* Jessica Silver-Greenberg, Matthew Goldstein & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES: DEALBOOK (Oct. 2, 2014, 12:50 PM), https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0.

[102] This is a hypothetical situation with no verifiable connection to actual facts or events. It is nonetheless completely plausible that such an individual exists given the size of the referenced breaches and the diverse industries each breach impacted, in which each company's products do not compete with the other companies' products.

[103] Judges have previously issued such limited discovery orders to establish standing. *See, e.g.*, Fla. Audobon Soc'y v. Brady, No. 90-cv-01195, 1990 WL 154297, at *1 (D.D.C. Sept. 27, 1990); *cf.* Am. Jewish Cong. v. Vance, 575 F.2d 939, 950 n.14 (D.C. Cir. 1978) (Robinson,

that his data was hacked in the Anthem and JPMorgan Chase incidents. With this information now known to the parties and the court, is it possible for Vince to carry his burden of proving the *causation* element of standing?[104]

Now, to be sure, Victim Vince is a very sympathetic plaintiff who, it seems, was clearly wronged and thus is deserving of *some* remedy. So, let us take the flip side of this hypothetical. Now, imagine that the onslaught of scholarly attention focused on surmounting the injury-in-fact hurdle, coupled with judges becoming more and more familiar with the unique harms associated with data breaches, has left plaintiffs far more likely to prevail against a challenge to the injury-in-fact prong.

With the work of some ingenious lawyering, Victim Vince had to change his name to Victorious Vince because every time his data is breached, he's able to sue the breached entity, survive the standing inquiry, and win.[105] The common remedy offered to data-breach victims is a year or two of credit monitoring.[106] If Vince's data were to be subject to hacks on three separate occasions within a year, given his new winning ways, it appears that he will be compensated with credit monitoring three times covering the same time period. This is an inefficient allocation of resources and runs counter to a bedrock legal premise that a remedy ought not overcompensate the victim.

The problems that inhere in the current approach to data breaches are threefold. First, despite the commonsense perception that data breaches cause real-world harm,[107] the standing hurdle prevents victims from seeking redress both now and in the foreseeable future. Next, given the remedy usually awarded in data-breach settlements, resolving this problem may likely result in an inefficient distribution of that remedy. But lastly and most concerningly, waiting for courts to recognize data breaches as harm-causing events is untenable. That is, given the prevalence and frequency of data breaches today, by the time courts

III, J., dissenting) ("Of course, if the facts on standing are uniquely within the knowledge or control of the opponent, limited discovery might be appropriate.").

[104] Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992) ("The party invoking federal jurisdiction bears the burden of establishing these elements.").

[105] Vince has, in fact, adopted as his motto "All I do is win win win no matter what!" DJ KHALED, ALL I DO IS WIN (Entertainment One Music 2010).

[106] *See, e.g.*, Settlement Agreement and Release, *supra* note 20, at 17 (stating that defendants must provide credit services to class members, including daily credit monitoring, identity validation monitoring, and internet surveillance); JOHNSON & MILLETT, *supra* note 5, at 11-13 (discussing California law requiring provision to data-breach victims of one year of identity theft prevention and mitigation when Social Security number is exposed).

[107] During a recent hearing in the House Committee on Financial Services, Representative Katie Porter questioned new Equifax CEO Mark Begor and demonstrated the absurdity of the argument that data breaches do not, in fact, cause harm. *See* Video Clip, *Rep. Katie Porter Asks Equifax CEO to Release His Social Security Number*, C-SPAN (Feb. 26, 2019), https://www.c-span.org/video/?c4782321/rep-katie-porter-asks-equifax-ceo-release-social-security-number [https://perma.cc/Z2XJ-MHG6].

begin to recognize these harms, society will suffer an untold quantum of damage that will not be remedied. This is in large part due to the fact that courts must take a piecemeal, individual, event-focused approach because they can only act on the case before them. Instead, using historical analogues as a guide, incentives to protect data must change and a new remediation system must be employed.

II. HISTORICAL RESPONSES TO PUBLIC RISKS

Analyzing the data-breach problem as a generalized, widespread public risk—instead of from the current, incident-centered perspective—enables more effective analysis of what the law can do in response to the problem. This alternative perspective avoids the pitfalls of overly narrow solutions, such as only protecting data in certain contexts,[108] by conceptualizing data privacy harms as a discrete, separate type of injury in need of effective legal redress.[109] History can serve as a guide towards crafting a new regime that is capable of effectively addressing the numerous issues inherent in data breaches by modifying incentives to make breaches less likely and providing redress for discrete incidents when they inevitably still occur. This Part will examine two historical responses to widespread public risks—the Vaccine Injury Compensation Program and the Federal Deposit Insurance Corporation—gleaning insight into the features, best practices, and potential pitfalls that may arise in a specialized data-breach legal regime. The lessons from this historical analysis will then be applied to data breaches, identifying the policy concerns that are likely to arise in a new program to address data breaches.

A. *Vaccine Injury Compensation Program*

The development of vaccines to prevent harmful diseases was a monumental scientific discovery that provided many benefits to society.[110] These vaccines, however, also resulted in a number of serious injuries and illnesses after inoculation, such as paralytic polio, anaphylaxis, and Guillain-Barré

[108] The law provides for more robust protection in several industries—and with good reason—because these fields maintain records with particularly sensitive data. *See, e.g.*, 15 U.S.C. §§ 6801-6827 (2012) (Gramm-Leach-Bliley Act covering financial institutions); 42 U.S.C. § 17931 (2012) (Health Information Technology for Economic and Clinical Health Act); 45 C.F.R. §§ 160.103, 164 (2014) (regulations under Health Insurance Portability and Accountability Act of 1996, covering many healthcare industry organizations).

[109] *See* Calo, *supra* note 48, at 1133 ("By delineating the specific boundaries of privacy harm, this Essay furnishes a defensible means by which to rule out and recognize privacy harms.").

[110] *See* Efthimios Parasidis, *Recalibrating Vaccination Laws*, 97 B.U. L. REV. 2153, 2154 (2017) ("[T]he health benefits of vaccines cannot be questioned seriously . . . .").

Syndrome.[111] Congress was presented with a dilemma. Vaccines provided, and continue to provide, critical public benefits that make our world a safer, healthier place. Yet, this unquestionable public benefit produces, to a high degree of statistical certainty, a number of serious harms. In order to "achieve optimal prevention of human infectious diseases through immunization and to achieve optimal prevention against adverse reactions to vaccines,"[112] Congress passed the National Childhood Vaccine Injury Act of 1986 ("the Vaccine Act").[113]

This statement of purpose, while straightforward on its face, was rife with latent issues and policy concerns. As Professor Efthimios Parasidis explains in great detail, several incidents with early vaccines from the 1950s through the 1980s produced a number of significant policy and legal challenges that the Vaccine Act sought to remedy.[114] First, there were questions surrounding how the parents and guardians of injured children would be able to demonstrate causation as part of a tort claim seeking redress for their children's injuries—what evidence would show that a vaccination and not some other source created the harm?[115] Next, after a series of issues with vaccines, the federal government indemnified "Swine Flu vaccine manufacturers, distributors, and administrators" during the Swine Flu outbreak in the 1970s.[116] The government created a federally funded compensation fund to remedy injuries arising from the immunization program, but after administrative and judicial liability claims nearly cost as much as the vaccine itself, the federal government knew it needed a different solution going forward.[117] These high litigation costs underscored the value that indemnification provided to vaccine manufacturers, but they also justified as reasonable the concern among manufacturers that vaccines may not be a financially sound business if profits would be subsumed by litigation costs and damage payments.[118] Each of these concerns either was addressed via the

[111] *See* 42 C.F.R. § 100.3 (2017) ("Vaccine Injury Table"—listing several of the most common illnesses, disabilities, injuries, or conditions covered by the National Childhood Vaccine Injury Act of 1986, codified as amended at 42 U.S.C. §§ 300aa-1 to -34). Something that bears repeating—vaccines do *not* cause autism. *Vaccines Do Not Cause Autism*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/vaccinesafety/concerns/autism.html [https://perma.cc/829A-WAVL] (last visited Aug. 22, 2019) ("There is no link between vaccines and autism.").

[112] 42 U.S.C. § 300aa-1 (2012).

[113] *Id.* § 300aa.

[114] *See generally* Parasidis, *supra* note 110.

[115] *Id.* at 2166 (stating that from 1950s through 1980s, courts were divided on "contours surrounding the causation elements of a negligence claim").

[116] *Id.* at 2196.

[117] *See id.* at 2199-200.

[118] *See id.* at 2208 ("Litigation risks—particularly when coupled with unpredictable manufacturing costs and revenues—led manufacturers and investors to question whether vaccines were financially worthwhile . . . .").

Vaccine Act or played an important role in understanding the final form of the legislation.

The Vaccine Act contains several pieces that, taken together, address these policy challenges. The Vaccine Act created the National Vaccine Injury Compensation Program ("VICP") to make payments to remedy vaccine-related injury or death, called "adverse events."[119] Funding was supplied via a seventy-five cent excise tax per vaccine dose, paid by the recipient of the vaccine, and directed to the Vaccine Injury Compensation Trust Fund ("Trust Fund") to cover the cost of the VICP, including both compensation and administration.[120] This meant that neither Congress nor the Treasury would be footing the bill, as was the case after the Swine Flu outbreak. Recognizing that the petitioners would be parents aggrieved by the death or serious injury of a child, Congress sought to make the Vaccine Injury program generous with its damage awards[121] and less adversarial.[122] Additionally, the VICP implemented a structure whereby certain adverse events, occurring within a certain time frame after inoculation, would be listed on a decision aid called the Vaccine Injury Table ("Table"). The Table allowed for a significant legal benefit—causation would be presumed for on-Table events, whereas other types of adverse events or events occurring outside the prescribed timeframe would be considered off-Table events for which the petitioner must undertake the arduous task of demonstrating causation.[123] The VICP also set forth certain categories of damages available to successful petitioners.[124] This was critical, after the enormous Swine Flu litigation damage totals, to ensure that the VICP's Trust Fund would not be overextended. Lastly, the Vaccine Act granted broad immunities to vaccine manufacturers with the hopes of encouraging innovation and a stable vaccine supply.[125]

For all its promise, however, many of the program's goals have failed to materialize in practice and to keep up with the rapid pace of scientific and medical advancement.[126] Despite its nonadversarial aims, a mere three years

[119] *Id.* at 2210.

[120] *Id.* at 2210-11.

[121] *See id.* at 2238.

[122] Nora Freeman Engstrom, *A Dose of Reality for Specialized Courts: Lessons from the VICP*, 163 U. PA. L. REV. 1631, 1711 (2015) ("Both the VICP and health courts aim to quell the adversarialism of dispute resolution.").

[123] *See* Parasidis, *supra* note 110, at 2215.

[124] *See id.* at 2216.

[125] *See* 42 U.S.C. §§ 300aa-21 to -23 (2012) (discussing damages in civil action against vaccine manufacturer); Bruesewitz v. Wyeth LLC, 562 U.S. 223, 243 (2011) (holding that "[Vaccine Act] pre-empts all design-defect claims against vaccine manufacturers brought by plaintiffs who seek compensation for injury or death caused by vaccine side effects"); Parasidis, *supra* note 110, at 2166 ("[T]he swine flu program led manufacturers to demand indemnification from the government for all vaccine-related injuries.").

[126] *See* Engstrom, *supra* note 122, at 1674-98; Parasidis, *supra* note 110, at 2154 ("Although the Vaccine Act may have been the cure for the vaccine woes of the 1980s, the

after the Vaccine Act was passed, "Congress expressed regret that, despite [the] statutory directive, 'all participants ha[d], to some degree, maintained their traditional adversarial litigation postures.'"[127] This is further demonstrated, sadly and ironically alongside the VICP's lack of generosity, in a case where the government contested a fourteen-year-old's need for forty-dollar high-top tennis shoes despite her "profound mental retardation and severe spastic quadriplegia."[128]

The liability immunity offered to vaccine manufacturers also deserves attention. Fear of substantial litigation costs drove the price of some vaccines sky-high, and drove some manufacturers to exit the market.[129] In an attempt to assuage these concerns and stabilize the market for vaccines, the Vaccine Act placed "'significant' limits on civil claims" against both doctors administering vaccines and the firms that manufacture them.[130] Not only must petitioners first proceed through the administrative adjudication offered under the VICP, but should a petitioner choose to seek traditional tort damages instead, the VICP also dramatically whittled down the types of claims and remedies available.[131] The Vaccine Act removes liability, in most cases, for: failure to warn; intentional addition of adulterants or contaminants; and choice of a particular design, despite the availability of a safer and equally effective design.[132] Furthermore, manufacturers are immune from punitive damages.[133] Despite pretextual arguments that this insulation from liability was necessary to promote innovation by allowing companies to shift funds from litigation expenses to research and development, it appears that such broad liability protection was merely a handout flowing from significant industry-lobbying efforts.[134] This is not to say that any immunity whatsoever is unnecessary or ineffective in

law has failed to keep pace with technological advancements and evolving public policy concerns.").

[127] *See* Engstrom, *supra* note 122, at 1712 (explaining that "system's adversarial nature has endured").

[128] Parasidis, *supra* note 110, at 2160 (citing Engstrom, *supra* note 122, at 1692) (providing examples of VICP disputes where "government quibble[d] over minor requests").

[129] *See* Engstrom, *supra* note 122, at 1657 (explaining how increased liability "spooked" some manufacturers).

[130] *See* Parasidis, *supra* note 110, at 2219.

[131] *See id.* at 2219-21 (explaining immunities and presumptions that benefit manufacturers facing litigation).

[132] *See id.*

[133] *See id.* at 2219.

[134] *See id.* at 2232 ("[T]he provision of the Vaccine Act that broadly preempts design defect claims addressed a non-issue (in terms of litigation-influenced market destabilization), and can be seen as a political handout to manufacturers who lobbied for 'greater insulation from liability.'" (quoting Engstrom, *supra* note 122, at 1659)).

stabilizing the vaccine market—some liability protection may be important.[135] But a statutory provision that "fails to ensure that manufacturers incorporate scientific advancements into vaccine design,"[136] as noted by Justices Sotomayor and Ginsburg in dissent in *Bruesewitz v. Wyeth LLC*,[137] surely needs to be reconsidered.

B. *Federal Deposit Insurance Corporation*

The Federal Deposit Insurance Corporation ("FDIC") presents a different type of solution to a different type of societal risk. As the name suggests, the FDIC is an insurance-based scheme protecting deposit accounts (i.e., checking, savings, money market accounts, and certificates of deposit, but not investment accounts) for losses up to two hundred fifty thousand dollars.[138] This program was initiated after some 9,096 banks failed between 1930-1933, resulting in bank customers sustaining a collective loss of nearly 1.3 billion dollars.[139] Given the post-depression cash crunch, funding this insurance program on the backs of the individuals working to get back on their feet was not a viable option. Instead, the Banking Act of 1933 initially funded the FDIC with contributions from the Treasury and the twelve Federal Reserve Banks.[140] Today, the program is funded through "premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities."[141] Banks initially paid a flat-rate premium of twenty-three cents per one hundred dollars of deposits.[142] This changed to a risk-based premium under the Federal Deposit Insurance Corporation Improvement Act of 1991, an "important step"[143]

[135] Pharmaceutical companies may need some liability risk in order to be actually incentivized to incorporate the safest available effective design. *See id.* But, more limited protections that keep manufacturers in the market without completely eviscerating incentives seem more appropriate. *See id.* at 2231 (discussing proposed statutory amendment to adjust liability protections while largely leaving those protections in place).

[136] *Id.* at 2231.

[137] 562 U.S. 223, 250 (2011) (Ginsburg & Sotomayor, JJ., dissenting) ("[The majority's] decision leaves a regulatory vacuum in which no one ensures that vaccine manufacturers adequately take account of scientific and technological advancements when designing or distributing their products.").

[138] Kathryn Judge, *Three Discount Windows*, 99 CORNELL L. REV. 795, 828, 828 n.200 (2014) (citing Dodd-Frank Wall Street Reform and Consumer Protection Act § 335, 12 U.S.C. § 1821(a)(1)(E) (2012)).

[139] DIV. OF RESEARCH & STATISTICS, FED. DEPOSIT INS. CORP., A BRIEF HISTORY OF DEPOSIT INSURANCE IN THE UNITED STATES 21 tbl.5 (1998).

[140] *Id.* at 27-28.

[141] *Who Is the FDIC?*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/about/learn/symbol [https://perma.cc/V7U7-YRLK] (last visited Aug. 22, 2019).

[142] Marcia Millon Cornett, Hamid Mehran & Hassan Tehranian, *The Impact of Risk-Based Premiums on FDIC-Insured Institutions*, 13 J. FIN. SERVS. RES. 153, 153-54 (1998).

[143] *Id.* at 154.

that helped to "align the incentives of [bank] owners and managers with the interests of the insurance fund."[144]

Given the program's structure as an insurance pool, high-risk banks (those that are undercapitalized, for example) pay higher premiums. Just as a teenage male driver pays more money for his car insurance because the insurance company knows he will pose a greater-than-average risk to the insurance fund, banks that are undercapitalized or poorly managed pay larger premia.[145] To be sure, the risk-based system is not immune to criticism, and it may be far from perfect.[146] Nevertheless, the move to risk-based premia helped to realign bank managers' incentives because "[r]isky institutions would internalize the costs of their risk-taking."[147]

The FDIC serves several important policy goals that benefit both financial institutions and consumers. From an institutional perspective, deposit insurance's primary aim is "to improve bank stability by discouraging runs [on banks]."[148] Underlying this sought-after stability is consumer confidence in the banking system. A bank run occurs when, fearing that their bank may be insolvent, customers flock to the bank in an attempt to withdraw deposited funds. "Because depositors who are first in line get paid in full while those who delay can end up receiving something less than the full amount the bank owes them," it was critical to buoy consumer confidence.[149] Indeed, in his first "fireside chat" President Franklin D. Roosevelt emphasized that the financial system relies most heavily, not upon currency or gold, but upon "the confidence of the people."[150]

---

[144] *Id.* (quoting Richard Scott Carnell, *The Culture of Ad Hoc Discretion*, *in* ASSESSING BANK REFORM: FDICIA ONE YEAR LATER 116 (George G. Kaufman & Robert E. Litan eds., 1993)).

[145] *Cf.* Shih-Cheng Lee, Chien-Ting Lin & Ming-Shann Tsai, *The Pricing of Deposit Insurance in the Presence of Systematic Risk*, 51 J. BANKING & FIN., Feb. 2015, at 1, 1 ("As a young driver who is characterized with high risk behind the wheel attracts higher insurance premium, a bank with higher failure risk pays a higher actuarially fair deposit insurance premium for the expected cost to the insurance provider.").

[146] *See, e.g.*, Cornett, Mehran & Tehranian, *supra* note 142, at 154 ("[T]he risk-based insurance premiums instituted in September 1992 may not have perfectly priced the risk imposed on the FDIC by banks . . . ."); Lee, Lin & Tsai, *supra* note 145, at 1 (explaining that banks' investments may be highly correlated, resulting in joint bank failures and that current insurance premium calculations fail to capture this risk).

[147] Cornett, Mehran & Tehranian, *supra* note 142, at 154 (quoting Richard Scott Carnell, *The Culture of Ad Hoc Discretion*, *in* ASSESSING BANK REFORM: FDICIA ONE YEAR LATER 116 (George G. Kaufman & Robert E. Litan eds., 1993)).

[148] Judge, *supra* note 138, at 828.

[149] *Id.*

[150] DIV. OF RESEARCH & STATISTICS, *supra* note 139, at 1 (quoting Franklin D. Roosevelt, President of the United States, The First "Fireside Chat"—An Intimate Talk with the People of the United States on Banking (Mar. 12, 1933), *in* 2 THE PUBLIC PAPERS OF FRANKLIN D. ROOSEVELT: THE YEAR OF CRISIS, 1933, at 65 (1938)).

There was strong public support for a federal plan to protect bank depositors,[151] and the deposit insurance system responded to the concerns of those individuals. Consumer protection was a key feature of the Banking Act in 1933, and it "remains a core concern animating many aspects of banking regulation."[152] The deposit insurance system furthers both perspectives, by providing for efficient monitoring.[153] The average individual bank customer does not have the economic expertise to evaluate a bank's financial health, and attempting to monitor a given bank's health "would be exceptionally time consuming."[154] Instead, the public can rely on "specialized regulator[s] who can more efficiently monitor and discipline the bank," which, in turn, reduces the monitoring costs necessary to an insurance regime.[155]

C. *Policy Lessons*

The above examples yield valuable lessons for designing a scheme to address data breaches. Given the dearth of paths to a post-breach remedy that plagues the legal system today, even a modest improvement would be a welcome change. The first takeaway is that both companies and individuals benefit from spreading the risks of substantial losses, whether those losses are litigation expenses and damage payments or the inability to withdraw money from the bank. In order to pay for the remedies necessary in the vaccine context, the Vaccine Act used excise taxes and established the Trust Fund as a core pillar of the VICP.[156] Similarly, through the FDIC, Congress removed the risk of loss from individual depositors by insuring their deposits up to a certain amount.[157] Given the massive litigation risk facing breached organizations, and the effectively judgment-proof international actors frequently involved in these incidents, a stable and diversified source of compensation would fulfill several goals. First, relying on an insurance model would spread the impact of any single breach more effectively in the market by taking the risk off of an individual company. The world of data security is perhaps less susceptible to such calculations than the world of banking, because "cyber risk is very different from the traditional

[151] *Id.* ("[P]ublic opinion remained squarely behind the adoption of a federal plan to protect bank depositors.").

[152] Judge, *supra* note 138, at 828.

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] Parasidis, *supra* note 110, at 2210-11 ("Vaccinees pay the [excise] tax, and vaccine manufacturers transfer the payment into the Trust Fund.").

[157] DIV. OF RESEARCH & STATISTICS, *supra* note 139, at 1 (noting that initial coverage limit was $2500 in 1934); *Who Is the FDIC?*, *supra* note 141 (noting that current coverage is at least $250,000).

risks covered by indemnity insurance,"[158] yet the existence of data-breach insurance indicates that such calculations are, in fact, possible.[159] Next, it would reassure individual victims that there is a real chance of receiving compensation for the injuries they sustain if their information is breached.

Reassuring victims of viable means of redress additionally supports the next policy goal of a new data-breach regime—increased consumer confidence. While confidence in data-reliant companies may not be as big of a concern as it was during the Bank Holiday of 1933, we have reason to believe it is of concern to modern consumers. That is, when given a choice, consumers take actions to protect their data. This can be seen through two separate events. First, when President Trump announced that his "Commission on Election Integrity" would seek voter data from the states, scores of individuals unregistered in an attempt to safeguard their data.[160] Later, after it was revealed that a company called Cambridge Analytica had retained data on some fifty million Facebook users, the hashtag #DeleteFacebook trended across the internet.[161] While users may not be ready to actually leave the social media site just yet,[162] the incident does demonstrate that a growing number of people are actively concerned with the security of their data. A regime that incentivizes companies to act more carefully with sensitive consumer data will rationally increase the aggregate level of data

[158] MAOCHAO XU & LEI HUA, SOC'Y OF ACTUARIES, CYBERSECURITY INSURANCE: MODELING AND PRICING 4 (2017).

[159] Given that data-breach policies are offered by large insurance companies well known for other more common forms of insurance, it is safe to assume that these companies have found a way to underwrite the policies in a profitable manner. *See, e.g.*, *Small Business Data Breach Insurance*, TRAVELERS, https://www.travelers.com/small-business-insurance/data-breach-insurance [https://perma.cc/38Q8-NB2U] (last visited Aug. 22, 2019);*Data Breach and Cyber Liability Insurance*, HARTFORD, https://www.thehartford.com/data-breach-insurance [https://perma.cc/RA9T-SGZE] (last visited Aug. 22, 2019).

[160] Dylan Wells & Saisha Talwar, *Some Voters Unregistering After Trump Administration's Data Requests*, ABC NEWS (July 14, 2017, 6:20 PM), http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555 [https://perma.cc/A6U5-D2UY] ("Three thousand, three hundred and ninety-four Coloradans have withdrawn their voter registrations as of July 13, following the Trump administration's request for voter data as part of the Commission on Election Integrity.").

[161] Jessica Guynn, *Delete Facebook? It's a Lot More Complicated than That*, USA TODAY (Mar. 29, 2018, 12:30 PM), https://www.usatoday.com/story/tech/news/2018/03/28/people-really-deleting-their-facebook-accounts-its-complicated/464109002/ [https://perma.cc/3ZXR-NPNY].

[162] *Id.* (noting that few users may leave given that there are "few good alternatives" to popular site); *see also* S. Shyam Sundar et al., *Why It's So Hard to #DeleteFacebook*, SCI. AM. (Mar. 28, 2018), https://www.scientificamerican.com/article/why-its-so-hard-to-deletefacebook/ [https://perma.cc/MSV6-BC3M] ("This flareup is a big one to be sure, leading some people to consider leaving Facebook altogether, but the company and most of its over 2 billion userswill [sic] reconcile.").

security employed by data-retaining entities, which may in turn increase consumer confidence in those firms' services.

Next, tools need to be in place to give aggrieved parties a more expedient path to a remedy. In the VICP context, that tool was the Injury Table, offering some reprieve to parties who would otherwise bear the nearly insurmountable burden of demonstrating the vaccine caused their injuries.[163] In the data-breach context, a series of factors impact the likelihood that one will ultimately suffer financial loss or identity theft. A tool that draws these factors to the attention of courts, along with a reasoned way to understand how significant each factor is, would go a long way to ensure that breach victims see adequate compensation. With a presumption of harm in certain, more severe circumstances, courts would cease to be bogged down in attempting to capture intangible, long-term harms. For data that is less sensitive, like a single payment method, a burden-shifting scheme placing the onus back on the plaintiff to demonstrate what harm they sustained would ensure that valuable resources are not being wasted on trifling injuries.

Lastly, immunity for entities that are breached despite implementing some standard data protection tools may help incentivize those entities to implement rigorous data-security measures. Vaccine manufacturers received nearly complete insulation from liability, which has proved to be a bridge too far.[164] In the data-breach context, there are surely some incidents where breached organizations were negligent in failing to implement adequate security measures. Yet, there are just as surely a number of organizations that are breached despite their attentiveness to data-security issues—firms that made a good-faith attempt to protect customer data that nevertheless fell victim to a particularly virulent cyberattack. Treating those firms equally produces bad incentives: If the firm is going to face liability regardless of implemented security techniques, why invest in data security at all? Thus, a different approach that strikes the right balance, unlike the Vaccine Act, will provide the proper incentives for firms to protect customer data from loss in the first instance.

III. A NEW SOLUTION:THE DELINEATED APPROACH TOWARDS ADDRESSING DATA BREACHES

Data breaches are a unique problem that demand a unique solution. This Part sketches the outlines of a new approach to handling data breaches—what this Note will refer to as the DATA-DB.[165] This comprehensive program, spreading

[163] Parasidis, *supra* note 110, at 2215.

[164] *See supra* notes 119-25 and accompanying text (discussing VICP damages regime).

[165] Given the intricate nature of a program that implicates highly technical cybersecurity principles; regulates a wide swath of U.S. commerce; works in tandem with a number of existing data privacy laws, see *supra* note 108 (citing statutes); and redirects some not insignificant portion of federal litigation to an administrative regime, much of the details necessary to a final proposal are beyond the scope of this Note (for example, the economic

responsibility across several pre-existing agencies, presents a dynamic and multifaceted approach to address a litany of issues: data security guideline formulation, development, and adoption; industry-specific responsiveness concerns; individual injury redress and compensation; and corporate risk and loss, including both primary and secondary parties.[166] The DATA-DB, at bottom, aims to modify incentives in order to reduce the incidence of data breaches, and to make data-breach victims relatively whole again after a breach occurs.[167] This process begins by setting incentives to ensure that the lowest cost avoiders—entities that maintain data reservoirs—are implementing data protection commensurate with the sensitivity of the data stored and keeping that protection updated to ward off new threats.

A. *Elements of the New Program*

DATA-DB requires several elements in order to address the multitude of issues presented by modern data breaches. The elements offered herein are guiding principles designed to present a more comprehensive response to this growing societal harm. That being said, this Note does not purport to identify the precise contours of DATA-DB. Many of the elements identified in this Section will undoubtedly require substantial future research before they are "implementation-ready." Economists will need to analyze the feasibility of the funding mechanism and set the data tax levels appropriately.[168] Data security experts will need to modify the standard-setting approach to ensure standards advance at an appropriate rate, which can be challenging given the pace of technological innovation, counterbalanced by the slow-moving nature of government processes. Public policy experts and industry experts will need to consider the implementation of DATA-DB within existing government agencies, like the Department of Health and Human Services or the Securities and Exchange Commission, which already regulate data within specific industries. Yet, combining these elements properly will produce an end result greater than the sum of its component parts—a viable, coordinated solution to

matter of how much money the DATA-DB would require and what the income would look like from the proposals in Section III.B, *infra*). Some work is already being done that will help to flesh out these ideas and fill in critical details. *See, e.g.*, U.S. Dep't of Health & Human Servs., *Data Privacy in the Digital Age—Panel 3: Privacy Policy and Regulation*, YOUTUBE at 36:02-47:05 (Nov. 13, 2017), https://youtu.be/LDLJgSiLZFw?t=2162 (discussing data privacy in healthcare context).

[166] *See supra* notes 65-70 (discussing various classes of parties impacted by breaches).

[167] Here, making the victim entirely whole would require returning now-disclosed information to its previous condition—confidential. This is not possible, so protecting the parties from the harms flowing from that disclosure is the best practically available remedy to make the victim relatively whole.

[168] For more on funding, see *infra* Section III.B.

minimizing the incidence and impact of data breaches on American consumers, industry, and government.

1. Standard-Setting Authority

Firms should be expected to comply with a rudimentary set of data-protection measures that are mandatory, cheap to implement, and easy to maintain. Presently, the Federal Trade Commission ("FTC") uses § 5 of the Federal Trade Commission Act (the "FTCA"), 15 U.S.C. § 45 (2012), to prosecute firms that fall woefully short of reasonable data security standards.[169] Yet, by setting the bar for enforcement so low, businesses are hardly incentivized to maintain adequate data security measures. Furthermore, the FTC has thus far only brought action under the purview of "unfair competition."[170] That is to say, the standard of which data practices rise to such a level is left largely unclear. This lack of clarity resulted in a robust challenge to the FTC's authority to regulate data security in *FTC v. Wyndham Worldwide Corp.*[171]

Much to the chagrin of defendants like Wyndham Worldwide Corp., which asserted that the FTC can only act in the data privacy space through more specific regulations, courts have held otherwise.[172] At the core of Wyndham's concern with FTC action under the remarkably elastic formulation "'acts or practices in or affecting commerce' that are 'unfair' or 'deceptive'" is the issue of notice.[173] In its brief, Wyndham noted that other administrative agencies, including the Department of Homeland Security and the National Institute of Standards and Technology, have developed data-security rules.[174] Again, while this did not have an impact on the FTC's legal duties and obligations as applied

[169] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2230 (2015) ("[T]he FTC has been quite modest in its enforcement, focusing on the most egregious offenders and enforcing the most widespread industry norms."); *see, e.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014) ("The Federal Trade Commission (the 'FTC') brought this action under Section 5(a) of the Federal Trade Commission Act . . . ."), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[170] *See, e.g.*, *Wyndham Wordlwide*, 10 F. Supp. 3d at 607 ("The FTC alleges that Wyndham violated Section 5(a)'s prohibition of 'acts or practices in or affecting commerce' that are 'unfair' or 'deceptive.'").

[171] *Id.*

[172] *See, e.g.*, *id.* at 620 ("Hotels and Resorts argues that, because the FTC has the power to issue particularized regulations and that it is plausible to do so, it *must*. . . . But the contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 'to the facts of particular cases arising out of unprecedented situations.'" (quoting FTC v. Colgate-Palmolive Co., 380 U.S. 374, 384-85 (1965))).

[173] *Id.* at 607 (quoting 15 U.S.C. § 45(a) (2012)); *id.* at 618 ("Hotels and Resorts insists that an agency 'has the responsibility to state with ascertainable certainty what is meant by the standards [it] has promulgated.'" (alteration in original) (quoting Dravo Corp. v. Occupational Safety & Health Review Comm'n, 613 F.2d 1227, 1232 (1980))).

[174] *See id.* at 620.

to that case, the point is well taken that it is practicable to promulgate such standards. Even if the slow-moving nature of rulemaking means that the standards lag slightly behind the forefront of state-of-the-art data-security practices, a lagging standard is better than no standard at all. Despite the apparent lack of a *legal* necessity to promulgate more specific regulations, such regulations would have the benefit of providing clearer lines and heightened requirements, thus producing the incentive effects to actually support compliance. Furthermore, if the FTC can enforce data security more robustly under its existing authorization, as Professors Hartzog & Solove maintain,[175] surely the FTC can enforce these newly articulated standards under DATA-DB. Though the FTC may presently possess the tools necessary to "develop more progressive data protection standards,"[176] the lack of such action indicates that perhaps a clearer statutory directive to undertake this important task is necessary.

2. Industry-Specific Specialization and Centralized Notification

Certain industries have peculiarly sensitive data,[177] and the law has recognized this by requiring several of these industries to adhere to more exacting standards.[178] DATA-DB is not meant to displace these long-implemented, more rigorous regimes. By providing for industry-specific specialization, DATA-DB will be able to help integrate the newly promulgated security standards, where appropriate, with existing laws. DATA-DB will provide further support to agencies, like the Department of Health and Human Services and the Securities and Exchange Commission, that play a role in administering these existing laws through enforcement actions.

Concurrently, DATA-DB will lead the way in regulating one of the most data-reliant industries—social media companies.[179] After the Cambridge Analytica data-scraping incident, Facebook CEO Mark Zuckerberg drew the ire of lawmakers in both the United States and Europe, many of whom called for regulations to constrain how the social media giant uses and protects customer

[175] Hartzog & Solove, *supra* note 169, at 2299 ("There is significant room in the broad domain marked out by Section 5 of the FTC Act for the FTC to expand its enforcement and develop more progressive data protection standards.").

[176] *Id.* (discussing FTC's hesitation in regulating data privacy).

[177] The sensitivity of particular data types is relevant in the funding context as well. *See infra* Section III.B.1 ("The first metric that the funding mechanism will take into account is the type of data that a firm retains.").

[178] *See supra* note 108 (citing statutes requiring more exacting standards with regard to sensitive data in certain industries).

[179] The FTC apparently agrees that such industry-specific regulation is necessary. *See* Cecilia Kang, *F.T.C. Members Prod Congress on Privacy*, N.Y. TIMES, May 9, 2019, at B3 ("Members of the Federal Trade Commission on Wednesday renewed their calls for Congress to create a national privacy law that would regulate how big tech companies like Facebook and Google collect and handle user data.").

data.[180] Social media has proved to be a treasure trove for advertisers, allowing social media companies to make a fortune. Yet, that data has the power to sway human behavior, and thus a stiff regulatory framework is critical to ensure that the data is not put to nefarious uses.[181]

Data-breach notification requirements are also a key regulatory device streamlined under DATA-DB.[182] Professor Cass Sunstein stated in 1999 that "*informational regulation*, or *regulation through disclosure*, has become one of the most striking developments in the last generation of American law."[183] Regulation through disclosure has played a critical role in the developing field of law related to data breaches and information security. In fact, it is one of the most common elements of existing state data privacy laws—the requirement that breached entities notify law enforcement agencies, consumer protection agencies, the consumer whose data was breached, or some combination of these groups.[184] Professors Paul M. Schwartz & Edward J. Janger have set forth six "dimensions" to maximize the benefit of data-breach notification laws.[185] In their proposed "Model Four" approach, a coordinated response agent ("CRA")

[180] Brian Barrett, *What Would Regulating Facebook Look Like?*, WIRED (Mar. 21, 2018, 9:55 PM), https://www.wired.com/story/what-would-regulating-facebook-look-like/ [https://perma.cc/SY97-WLY2] ("Thanks to repeated lapses from not just Facebook but all corners of Silicon Valley, some sort of regulation seems not only plausible but imminent."); Julia Carrie Wong & Sabrina Siddiqui, *Mark Zuckerberg Agrees to Testify Before Congress over Data Scandal*, GUARDIAN (May 25, 2019, 12:30 PM), https://www.theguardian.com/technology/2018/mar/27/mark-zuckerberg-testify-congress-cambridge-analytica-data-scandal [https://perma.cc/2VVF-SFFL] (noting that Zuckerberg agreed to testify in U.S. but sent other executives to testify in U.K.).

[181] As part of a pending settlement with the FTC, in an attempt to head off such regulation, Facebook has reportedly agreed to create a privacy committee. Cecilia Kang, *Facebook Set to Add Posts to Safeguard User Privacy*, N.Y. TIMES, May 2, 2019, at B1. This is on top of a potential record financial penalty. *See* Mike Isaac & Cecilia Kang, *Facebook Says U.S. Regulators Will Hit It Hard*, N.Y. TIMES, Apr. 25, 2019, at A1.

[182] Data-breach notification laws are, in and of themselves, a complex legal scheme that requires an intricate array of policy choices. The intricacies of those policy choices are beyond the scope of this Note, yet the need for a coordinated response is critical to both these laws and the DATA-DB.

[183] Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613 (1999).

[184] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 972-84 (2007) (listing information about various elements of state-level data-breach notification laws); *see also* BAKERHOSTETLER, DATA BREACH CHARTS (2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf [https://perma.cc/7K8R-8NAS] (summarizing various iterations of states' data-breach notification laws, including states that require notification to "Attorney General or State Agency").

[185] Schwartz & Janger, *supra* note 184, at 932 (enumerating six dimensions that shape data-breach notification regulations).

is "[c]entral" to a maximally effective data-breach notification policy.[186] DATA-DB would require entities that store data to designate a CRA and create a plan for disseminating notices in the event of a breach.

Intuitively, it seems to make sense that notifying individuals whose data was breached is sound policy because it allows individuals to mitigate the harm by securing their accounts, changing passwords, and placing freezes on their credit reports. Yet, data-breach notification laws rarely produce such behaviors among consumers,[187] and because notification has a substantial reputational cost to breached firms,[188] mandatory notification laws must strike a delicate balance.[189]

DATA-DB will help find that balance by creating a group within the FTC's Division of Privacy & Identity Protection[190] that will be tasked with crafting timelines for disseminating notices, developing sample notices aimed at each of the various parties to a given breach, and supplying this information to the CRA at a breached entity. Relying on the work of Schwartz, Janger, and others, this group can centralize knowledge related to effective notifications and serve to help ensure compliance with the current patchwork of state-level data-breach notification laws.

3. Efficient Dispute Resolution and Remedy Distribution

Requiring stronger data privacy protections is unquestionably the most urgent need addressed by DATA-DB, for adequate protections may be capable of substantially mitigating losses in the first place. Yet, as breaches inevitably occur, resulting in very real harms impacting the American public, a system that provides for real remedies is necessary. DATA-DB's Data Harm Adjudication Board ("DHAB") will have the authority to hear disputes arising from data breaches. Heeding the cautionary tales expressed in analyses of specialized dispute resolution processes,[191] DHAB can serve as the next frontier for alternative adjudicatory regimes by incorporating the various changes proposed by the literature in the pursuit of an elusive goal—a fair and fast resolution.

---

[186] *Id.* at 960 ("Central to the architecture is a coordinated response agent (CRA) that oversees steps for automatic consumer protection and heightens mitigation.").

[187] *See id.* at 949 (noting that early warning function of data-breach notification laws is "largely ineffective at present" in spurring consumer action).

[188] *See id.* at 935 (analyzing reputational information as type of sanction).

[189] *See id.* (taking deep dive into complexities of data-breach notification laws and proposing new approach).

[190] *Bureau of Consumer Protection Organization Chart*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/attachments/bureau-consumer-protection-organization-chart/bureau_of_consumer_protection_org_chart_1-30-19.pdf [https://perma.cc/F7JQ-ALHS] (last visited Aug. 22, 2019).

[191] *See* Engstrom, *supra* note 122, at 1698-715 (distilling analysis of VICP into lessons for alternative compensation mechanisms); Parasidis, *supra* note 110, at 2221-41 (proposing measures to modernize Vaccine Act to set better incentives and remedy issues with existing vaccine injury adjudication system).

Several features of DHAB will help make that goal a reality. First, specialized adjudicators fluent in the language of data forensics and cybersecurity are better able than common Article III judges to process the complex, technical data produced in breach investigations. Much like the VICP uses Special Masters,[192] DHAB can rely on Special Masters to produce findings of fact in disputes that are inherently esoteric. Consolidating the fact-finding process from the onset, as opposed to the multi-district litigation approach which cannot move forward until a number of claims are filed in federal courts across the country, should promote the efficiency of the resolution process.

Next, DHAB's adjudication approach will support business interests. When a business is found to have been employing heightened data-security protocols, it may be absolved of liability, thus morphing claims into a nonadversarial proceeding where both the breached entity and the individual whose data was disclosed can seek redress from the DHAB. This recognizes that firms are often victims, not culprits, when that firm is the target of a breach and that, consequentially, the firm ought not bear substantial litigation expense when it took reasonable steps to prevent the breach in the first place. This contrasts with firms that demonstrate a reckless disregard for customer data, to which the DATA-DB will offer no protection. Instead, beyond the fines imposed by the DATA-DB, regulatory agencies will be able to pursue more significant damages under other federal statutes.[193] Under either extreme, the breached entity is not an adverse party in relation to claims filed by harmed individuals. When the DHAB has verified that a breach has occurred, it can promptly contact impacted individuals notifying them of a right to compensation, much in the way that members in a class action receive a settlement notice. The key difference is that under DHAB, that notice comes shortly after the incident instead of after a protracted series of motions, discovery, and settlement negotiations. Finally, the DHAB can remit payments to classes of parties largely ignored in today's landscape, such as the banks that face costs in the wake of payment-system data breaches. A bank can aggregate data on how much it spent to generate new account numbers, distribute new cards, and perform other breach-related administrative functions. It can then submit that data to the DATA-DB to ensure that it is not forced to pay because of another firm's negligence or another actor's criminal invasion of a computer system.

The anecdote of Victim Vince turning into Victorious Vince illustrates the issue of inefficient remedy distribution—when an individual's data is breached multiple times, that individual should not be able to profit by collecting a remedy

[192] Parasidis, *supra* note 110, at 2159 n.32 ("Special masters are appointed by the Court of Federal Claims and are charged with adjudicating vaccine compensation petitions.").

[193] *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (denying corporate defendant's motion to dismiss FTC's action brought under Section 5 of FTCA).

from each breached entity.[194] If credit monitoring and protection is sufficient to provide a data-breach victim with security and peace of mind, such a remedy can be distributed more efficiently if done through a single administrator. The issue of excessive remedy distribution seems far afield given the current inability of data-breach victims to reliably establish a sufficient "injury in fact" for standing purposes.[195] Yet, with a regime that embraces the reality of the harms imposed by data breaches, this issue is likely to arise. Nevertheless, the DATA-DB is capable of "looking around the corner" and meeting challenges that are still beyond the horizon.

B. *Funding*

DATA-DB will require significant funding to compensate individual victims for the harms they suffer as a result of data breaches, to support data forensics investigations for hacked entities, and to fund enforcement activities undertaken against noncompliant data-retaining entities. Victim compensation will come from DATA-DB's Compensation Fund ("the Fund"), a trust fund-like arrangement where interests on the Fund balance generate the payments. Additionally, should a surplus accrue in the Fund, the money may be used to support grants to develop better data security practices that would become part of the public domain.[196]

To be sure, compensation funds are hardly a new innovation in the law. Beyond the VICP example explored in depth,[197] funds were created to compensate victims of the September 11 terrorist attacks[198] and workers injured on the job.[199] Victim funds have even been proposed in the data-breach context.[200] The Fund described here is only part of a larger program and, through interaction with other elements of the program, it is designed to serve additional goals. Beyond what may be referred to as the primary goal—compensating

---

[194] *See supra* notes 102-06 and accompanying text (discussing Victim Vince hypothetical).

[195] *See supra* notes 90-94 and accompanying text (discussing whether data breach constitutes "injury in fact" as it relates to establishing standing).

[196] *Cf.* Parasidis, *supra* note 110, at 2239-40 (proposing to reinvest VICP funds to support vaccine research).

[197] *See supra* Section II.A (discussing VICP).

[198] September 11th Victim Compensation Fund of 2001, Pub. L. No. 107-42, 115 Stat. 237 ("It is the purpose of this title to provide compensation to any individual (or relatives of a deceased individual) who was physically injured or killed as a result of the terrorist-related aircraft crashes of September 11, 2001.").

[199] *See generally* Richard A. Epstein, *The Historical Origins and Economic Structure of Workers' Compensation Law*, 16 GA. L. REV. 775, 776-79 (1982) (discussing historical origins of employer liability).

[200] Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get Over It!*, 19 SMU SCI. & TECH. L. REV. 3, 9 (2016) ("Another alternative to a private lawsuit is to create an administered compensation fund to compensate victims of breaches.").

individual victims—the Fund has the capability to redress harm to other parties like banks that incur data-breach-related costs. Furthermore, the Fund, as outlined here, corrects business incentives by producing a chilling effect on excessive data collection and transfers, which reduces individual data exposure. Simultaneously, civil fines for noncompliance with the data standards promulgated as part of the DATA-DB provide strong incentives for businesses to improve preventative security measures.

The funding mechanism needs to account for several factors. First, not all data is created equally. A mere list of usernames and passwords is far more innocuous than financial data or PII. Second, sensitive personal data today often moves from company to company, enabling many of the internet-based services we take for granted.[201] Yet, each of these transactions increases an individual's exposure to future breaches. These business-to-business data transactions need to be considered when devising a funding mechanism. Third, different organizations employ different types of data security, which may either increase or decrease the risk of that particular organization being breached. The funding mechanism should account for the different risk levels presented by firms employing different security measures. Conversely, firms should not be incentivized to go overboard with security measures—a startup that simply collects an individual's username, password, and a security question ought not feel as if the only way to avoid liability is to utilize bank-level security measures.

These factors will all be built into the funding mechanism, which will take on a few features of the VICP's excise tax model and a few features of the FDIC's risk-based insurance model. At bottom, the DATA-DB's Fund will be funded through several different sources. First, firms that retain certain types of customer data will pay a small tax for every user. Firms are accustomed to maintaining an accurate accounting of new and "daily active" users, as these data points are critical to firms' financial disclosures and pitches for new rounds of funding.[202] A small excise-type tax on users will ensure the fund remains viable. Next, when businesses sell blocks of customer data to other businesses, customer data is exposed to greater risk. Thus, to account for this increased risk, firms engaging in such types of transactions should compensate the Fund accordingly. Lastly, firms that fail to implement properly noticed security standards should be subject to substantial civil money penalties.

The first metric that the funding mechanism will take into account is the type of data that a firm retains. Data types will be placed on a continuum, ranging

[201] Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN (Aug. 23, 2012, 3:52 PM), https://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html [https://perma.cc/7HT6-H5GV].

[202] *See* App Partner, *The Quick & Dirty Formula for Calculating Your App Startup's Valuation*, MEDIUM (Aug. 16, 2017), https://medium.com/app-partner-academy/the-quick-dirty-formula-for-calculating-your-app-startups-valuation-4cd614da4e6f [https://perma.cc/EAN5-Y27Q] (considering factors such as number of users and user engagement in calculating technology company's prospective valuation).

from data that customers can reasonably be expected to manage on their own, such as passwords, to data that is impossible to change yet highly valuable to a hacker, such as one's date of birth, maiden name, or Social Security number. Much in the way that the FDIC adjusts insurance rates charged to a bank based on the bank's financial fundamentals and the bank's risk to the insurance pool, the DATA-DB will incorporate data type as an indicator of the potential for harm if that data is compromised in a breach.

Whole companies and industries today are founded on a revenue model that is based on the ability to either collect customer data and sell it or buy customer data and analyze it to make it more useful for others. To the extent that these types of transactions increase the exposure of an individual's data, a seemingly natural result of the same data being held in more "data reservoirs," companies should account for that risk in the form of a contribution to the Fund.

Lastly, after the DATA-DB sets standards for data security, inevitably some companies will fail to comply. While this result seems unavoidable, the use of civil penalties will serve several important purposes. First and foremost, the fines deter entities from retaining customer data without adequate security measures. Security auditing protocols, established as part of the standard-setting process, will empower regulators to ensure compliance with DATA-DB standards. Knowing that it may be audited, and that a failed audit results in a fine, covered entities will have an incentive to employ adequate data protection measures. Furthermore, these fines provide an additional revenue stream for the Fund. This makes sense from a risk perspective—firms with lax security practices present a greater risk to the remedy payment pool. So, those firms must internalize that risk through fines.

CONCLUSION

Data breaches have become a common occurrence in economies that continuously shift towards a greater reliance on bits and bytes. The proliferation of technology across industries as diverse as finance, healthcare, retail, and social media is not showing any signs of slowing down. Thus, the increasing frequency, size, and severity of data breaches will similarly continue to grow. Parties involved, from private companies to government organizations to the average American consumer are, at present, left with a system that inadequately incentivizes parties to maximize social welfare and that leaves parties of all types facing large, uncompensated losses.

When policymakers and lawyers pause and look at the problem of data breaches as a societal harm instead of a complicated series of discrete actions that results in some amorphous, intangible harm, real solutions begin to come into focus. To be sure, there is merit behind efforts with a short-term focus, like getting courts to recognize data-breach harms as "concrete" injuries that should open the doors of federal court. Ultimately, however, this problem is much too big for the judicial system to tackle alone. There are a number of different aspects to data breaches that ought to be dealt with proactively, before a breach even occurs.

The DATA-DB sets forth the outlines of a solution that is comprehensive and robust. Through pre-breach incentives and standard-setting authority, the DATA-DB can minimize the occurrence of breaches and mitigate the loss that results when a breach inevitably occurs. Then, through its modified adjudication structure, it can provide individuals with the relief they deserve while offering liability protection for data-collecting entities. As Schwartz and Janger assert, "[t]he legal system should do far more to protect [consumers] from the harms that flow from data breaches."[203] The DATA-DB offers that protection.

[203] Schwartz & Janger, *supra* note 184, at 971.