Maryland Law Review

Volume 82 | Issue 4 Article 4

Cybersecurity and Data Breach Harms: Theory and Reality

David W. Opderbeck

CYBERSECURITY AND DATA BREACH HARMS: THEORY AND REALITY

DAVID W. OPDERBECK*

This Article challenges the view among some privacy scholars that private law should routinely recognize dignitary, emotional distress, or potential future harms in commercial data breach cases. Such harms might be cognizable in specific and relatively rare circumstances, but they are not empirically or doctrinally viable in the mine run of cases. A realistic account of how commercial cybercrime works and how cybercriminals make money demonstrates that a reasonable person should not become excessively anxious upon receipt of a data breach notification. At this point in the history of cyberspace, commercial cybercrime is a systemic problem more than an individual one. Systemic solutions focused on strengthening data security provisions in comprehensive privacy laws, enhancing payment card security, updating fraud prevention measures related to credit reporting, and reforming aspects of the credit reporting and U.S. Social Security numbering systems should play a more important role than private litigation. A focus on anxiety-based harms in data breach cases, in contrast, would yield few cybersecurity benefits while distorting longstanding tort doctrines and transferring rents to class action lawyers.

* Professor of Law and Co-Director, Institute for Privacy Protection and Gibbons Institute of Law, Science & Technology, Seton Hall University Law School. Thanks to Derek Bambauer, Gus Hurwitz, James Cooper, Bruce Kobayashi, and Dan Solove for helpful comments on an earlier draft of this Article and to Kaitlin Principiato for excellent research assistance.

INTRODUCTION

Data breaches baffle legal scholars, economists, and courts. Nearly everyone believes that data breaches cause some harm to individuals whose data was improperly disclosed, but nobody seems to know just what that harm comprises or how the law should compensate victims.

Data breaches almost always involve a crime perpetrated by the individual or group that misappropriated the breached data.[1] Many of these

1. In the U.S., the Computer Fraud and Abuse Act ("CFAA") is the most directly applicable criminal statute. 18 U.S.C. § 1030. Some data incidents involving "insiders" might not trigger the

individuals and groups are beyond the reach of law enforcement, however, as they are often connected with international organized crime and nation-state actors.[2] Even when a criminal can be apprehended and prosecuted, individuals whose personal identifying information ("PII") was compromised usually cannot recover civil remedies. Individual cybercriminals ordinarily possess no assets against which a civil judgment realistically could be levied.[3]

When civil cases are brought, often as class actions, they proceed against the commercial entities holding consumer PII that are also the victims of the criminal breach.[4] Sometimes these cases are dismissed for lack of standing. When cases get past the hurdle of standing, sometimes they are dismissed on the merits for lack of duty, breach, causation, or related issues under the common law and consumer fraud statutes. Cases that traverse these initial hurdles may result in a class settlement.[5] The civil litigation landscape is highly unsettled and seems to be providing neither meaningful signals about deterrence and insurance nor compensation to individuals.

A core problem is that courts and commentators continue to envision data breaches as a homogeneous phenomenon through which individuals are victimized. Data breaches, however, are but one component of a larger cybersecurity and cybercrime ecosystem. Data breaches usually are preceded by other kinds of malicious cyber activity directed at commercial entities, such as retailers, website proprietors, and banks, that all hold significant amounts of consumer PII.[6] Some data breaches involve vulnerabilities that likely could have been corrected through seemingly minor fixes, such as patching older software. Other breaches result from attacks that seem more sophisticated, such as highly polished phishing campaigns or zero-day exploits.[7] A narrow focus on harms to individual consumers whose PII might

---

CFAA's "without authorization or exceeds authorized access" provisions. *Id.*; *see* Van Buren v. United States, 141 S. Ct. 1648, 1658–60 (2021). These incidents do not usually involve the large-scale exfiltration of consumer data, which is the concern of this paper. *See infra* Part I.

2. *See infra* note 29.

3. *See infra* Part I.

4. *See, e.g.*, Peter C. Ormerod, *Privacy Injuries and Article III Concreteness*, 48 FLA. ST. U. L. REV. 133 (2020) (discussing cases by individuals against commercial entities that suffered data breaches); David W. Opderbeck, Data Breach Consumer Class Action Settlements: Experience and Policy (Apr. 24, 2023) (unpublished manuscript) (on file with author) (describing class action settlements in cases by individuals against commercial entities that suffered data breaches).

5. *See* Opderbeck, *supra* note 4; *infra* Section I.C.

6. *See infra* Part I.

7. *See, e.g.*, VERIZON, DATA BREACH INVESTIGATIONS REPORT (2022), https://www.verizon.com/business/resources/reports/dbir/?cmp=knc:ggl:ac:wls:dpr:8888855284&utm_term=verizon%20data%20breach%20report&utm_medium=cpc&utm_source=google&utm_campaign=GGL_BND_Security_Exact&utm_content=DBIR2022&ds_cid=71700000082347933&gclid=Cj0KCQjwlemWBhDUARIsAFp1rLWFCla9iECckeRNB11UV_MouvfwShs3PmEgwh0GAVUYp2I84sDWWuAaAtBBEALw_wcB&gclsrc=aw.ds.

have been compromised because of a breach misses important facets of the broader cybercrime ecosystem.

Some commentators and authorities propose expanding remedies for privacy violations to include dignitary and emotional harms along with prophylactic remedies akin to medical monitoring damages.[8] On the surface, this seems to make sense. But there are serious doctrinal and evidentiary problems with such proposals.

Doctrinally, even in medical negligence and toxic tort cases, the state of the law is at best ambivalent concerning these remedies. This ambivalence is a feature, not a bug, of tort law. Tort law is not designed to impose enterprise-wide liability for general societal harms because the judicial system is neither institutionally capable of handling nor democratically accountable for addressing general societal harms. Some of this ambiguity relates to the evidentiary question of whether, or to what extent, exposure to a toxic substance increases a person's risk of some illness beyond the background risk where the substance is already present in some lesser degree.[9] The evidentiary question is at least as acute concerning specific uses of an individual's PII after any given data breach.[10]

This seems counterintuitive. We might assume that a data thief will use every piece of stolen PII from every individual data breach to make money in a way that economically harms every individual victim. That assumption would be wrong, for three reasons. First, much, if not most, of the PII taken in any given data breach will not be used for true identity theft or payment card fraud in ways that could affect the individual's accounts.[11] The secondary markets for consumer PII are diverse. Much of the pilfered PII available in these markets is not used for true identity theft or direct payment card fraud, but instead is used for synthetic identity fraud, which is not associated with a real person, or for other purposes such as espionage. Second, the secondary markets for consumer PII are vast and saturated. PII relating to nearly every American consumer is already available on the dark web from multiple breaches.[12] There is often no way to trace a specific

8. *See* AM. L. INST., PRINCIPLES OF THE LAW—DATA PRIVACY § 14(d), § 14 cmt. c, Westlaw (database updated Oct. 2020) [hereinafter ALI PLP]; Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 744 (2018) [hereinafter Solove & Citron, *Risk and Anxiety*]; Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) [hereinafter Citron & Solove, *Privacy Harms*].

9. *See infra* Section III.C.

10. *See infra* Part II.

11. *See infra* Parts II, III.

12. The "dark web" is not indexed by search engines such as Google and is accessible only through specialized web browsers that use encryption and other anonymization techniques. *See What is the Deep and Dark Web?*, KASPERSKY, https://www.kaspersky.com/resource-center/threats/deep-web (last visited Apr. 6, 2023).

fraudulent charge to the use of PII from a specific breach.[13] Third, in the vast majority of cases when an individual does suffer true identity theft or payment card fraud, the matter is swiftly rectified without cost to the consumer by credit providers, as required both by law and by the providers' agreements with the consumer.[14] Careful attention to where data breaches fit within the taxonomy of privacy harms therefore complicates the intuition that individuals should ordinarily have at least dignitary or prophylactic remedies against breached data processors and controllers.[15]

The jump to emotional, dignitary, and prophylactic remedies for individuals affected by data breaches also fails to weigh the benefits of the data collection and aggregation that are an inescapable part of life in cyberspace. One of the most significant is the credit benefit, which only exists because of large scale data processing and is worth hundreds of billions of dollars to the economy.[16] These benefits also involve some risks. In particular, the nature of the Internet means that some degree of leakage—some degree of cybercrime—is inevitable. But the value of the credit benefit is substantial. A reasonable person living in cyberspace will know that their PII will be used for these beneficial purposes, that this PII will never be completely secure, and that at least some of this PII will inevitably end up on the dark web—and the reasonable person will not become excessively emotionally distressed about these facts of life, even if they are unpleasant.

This is not to say that law enforcement should give up, that private law has no role to play in enhancing cybersecurity, or that there is no role for regulation. Every data breach causes harm, both to the breached entity and to society. It is enough to say, though, that emotional, dignitary, and prophylactic civil remedies for individuals affected by data breaches are unlikely to help anyone. More useful measures would include embedding stronger data security requirements in comprehensive privacy laws,

13. *See infra* Parts II, III.

14. *See infra* Parts II, III.

15. This Article uses the terms "data processor" and "data controller" because they became standard terms in privacy compliance through their use on the European General Data Protection Regulation ("GDPR"). A "data controller" is an entity that has authority to determine the use of PII—for example, to accept a credit card for the purchase of goods. *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) art. 4(7) ("controller"). A "data processor" is an entity that processes PII in accordance with the controller's instructions—for example, a third party credit card processor that enables a retailer to accept credit cards. *Id.*, art. 4(8) ("processor"). Under the GDPR, both controllers and processors have obligations to data subjects, although in some circumstances processors may owe lesser duties than controllers. *See id.*, art. 24, 28. Presumably the distinction between controllers and processors would not matter under a tort, contract, or property-based claim.

16. *See* William Roberds & Stacey L. Schreft, *Data Security, Privacy, and Identity Theft: The Economics Behind the Policy Debates*, 33 ECON. PERSP. 22, 24 (2009); *see also infra* Section I.C.

strengthening the risk spreading mechanisms in the global payment card system, updating fraud prevention measures related to credit reporting, and migrating the Social Security number system to a more secure digital format. Such measures would work alongside market incentives to help manage a problem that cannot be solved.[17]

Part I of this Article explains why cybercrime is a hard problem and how it complicates the taxonomy of privacy harms. Part I also discusses how the benefits of PII disclosure in cyberspace relate to the risks of exposure to cybercrime. Part II examines the significant doctrinal and evidentiary problems with dignitary, emotional, and prophylactic remedies for privacy exposures stemming from data breaches. Part III explores possible regulatory measures to address the systemic privacy-related harms of commercial cybercrime. A brief conclusion is offered in the final Part.

I. THE HARD PROBLEM OF COMMERCIAL CYBERCRIME AND THE RISKS AND BENEFITS OF LIFE IN CYBERSPACE

It is a cliché heard often at data security conferences: It's not a matter of "if" you will suffer a data breach, it's a matter of "when."[18] Although the cliché represents a healthy amount of FUD ("fear, uncertainty, and doubt") spreading by security consultants, lawyers, and others looking for business, it contains an element of truth.[19]

According to the most recent IBM "Cost of a Data Breach Report," the average total cost of a breach to the affected entity in 2022 was $4.35 million.[20] No commercial enterprise wants to suffer a data breach. Every commercial enterprise has market incentives to take protective measures against data breaches. But data breaches still happen with regularity.[21] Private entities sometimes can be faulted for basic cybersecurity mistakes, such as

17. *See infra* Part III.

18. *See, e.g.*, Paul Mee and Rico Brandenburg, *Cyberattack: Not If, But When*, OLIVER WYMAN, https://www.oliverwyman.com/our-expertise/insights/2017/sep/cyberattack-not-if-but-when.html; Tyler Anders et al., *Not "If" But "When"—The Ever Increasing Threat of a Data Breach in 2021*, K&L GATES (July 15, 2021), https://www.jdsupra.com/legalnews/not-if-but-when-the-ever-increasing-8569092/; David Barton, *When Will Your Data Breach Happen? Not A Question of If But When*, SEC. INFO WATCH (Mar. 10, 2015), https://www.securityinfowatch.com/cybersecurity/information-security/article/12052877/preparing-for-your-companys-inevitable-data-breach.

19. "FUD" is Fear, Uncertainty, and Doubt. The term was popularized by mainframe computing pioneer Gene Amdahl in the 1970s. *See* Martin Veitch, *RIP Gene Amdahl: Pioneer of Mainframe Computing*, IDG CONNECT (Nov. 13, 2015, 9:08 AM), https://www.idgconnect.com/article/3578817/rip-gene-amdahl-pioneer-of-mainframe-computing.html.

20. IBM, COST OF A DATA BREACH REPORT 5 (2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.

21. *See id.* (finding that 83% of organizations have had more than one data breach).

failing to implement software patches, not encrypting sensitive data, or not training employees about social engineering awareness. But in every case, the breached entity is also a victim of a crime.[22] And cybercrime is a hard problem that cannot easily be solved.

Commercial enterprises that suffer data breaches, of course, are not the only victims of cybercrime. Data breaches often involve the exfiltration of the PII of thousands, millions, or even billions of individuals.[23] It seems obvious that each of these individuals is also a victim and that, unlike the breached entity, the individual victim bears no fault at all. Our intuition is that such individual victims should be compensated by the entity that lost their data. But that intuition is not so obviously correct. First, we must consider what kind of privacy "harm" the individual has suffered—if any. Commercial cybercrime, when examined in detail, complicates recently proposed frameworks for assessing privacy harms.

A. Why Cybercrime Is a Hard Problem

Cybercrime is a hard problem because cybercriminals operate in a technologically and socially complex international ecosystem.[24] Not every individual cybercriminal is a brilliant hacker, but all of them have ready access to easily configurable infrastructure and toolkits. Cybercriminals often employ sophisticated infrastructure devices and services, including "bulletproof" hosting services that resist law enforcement detection, personal computers that have been compromised by prior attacks and linked to botnets, disposable commercial cloud services (called "living off the land"),

22. The basic computer crime law in the United States is the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The U.S. Department of Justice maintains a website of press releases regarding cybercrime cases. *CCIPS Press Releases – 2022*, U.S. DEP'T OF JUST. (July 25, 2022), https://www.justice.gov/criminal-ccips/ccips-press-releases-2022. *See generally* CROWDSTRIKE, 2023 GLOBAL THREAT REPORT (2023), https://go.crowdstrike.com/2023-global-threat-report?utm_campaign=globalthreatreport&utm_content=crwd-laqu-en-x-tct-us-psp-x-wht-gtre-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=cyber%20threat%20report&gclid=Cj0KCQjwlPWgBhDHARIsAH2xdNdYODHS89LAr2KnsG2gxwJ2X0vGBwtpsK2BxkDZi5ai7tzGwNJjlPIaAi6WEALw_wcB.

23. *See, e.g.*, Michael X. Heiligenstein, *Recent Data Breaches – 2023*, FIREWALL TIMES (Apr. 7, 2023), https://firewalltimes.com/recent-data-breaches/; Lily Hay Newman, *The Worst Hacks and Breaches of 2022 So Far*, WIRED (July 4, 2022, 7:00 AM), https://www.wired.com/story/worst-hacks-breaches-2022/; Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Nov. 8, 2022, 2:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

24. *See generally* Derek Manky, *Defeating the Organized Cybercrime Ecosystem*, SECURITYWEEK (July 13, 2021), https://www.securityweek.com/defeating-organized-cybercrime-ecosystem; CROWDSTRIKE, 2022 GLOBAL THREAT REPORT 2 (2022) (noting that, in 2021, "eCrime syndicates refined and amplified big game hunting (BGH) ransomware attacks that ripped across industries, sowing devastation and sounding the alarm on the frailty of our critical infrastructure").

encrypted browsers such as Tor, steganography,[25] anonymizing VPN services, and censorship bypassing services.[26] Many of these tools and services are provided by enterprises that also serve individuals and business for legitimate purposes, such as the protection of trade secrets or the promotion of civil liberties in repressive regimes.[27]

There is also a robust underground market in tools and services designed specifically for cybercriminals.[28] Programmers offer user-friendly, easily configurable malware kits for users who want to engage in denial of service, cyber spying, and data exfiltration campaigns.[29] Users can contract for Cybercrime-as-a-Service ("CaaS") offerings in which a provider carries out the deployment of malware on the user's behalf.[30] Most cybercrime services even feature the ability to leave starred reviews, provide dispute resolution services, and offer other accoutrements of legitimate e-commerce sites.[31]

Any response to cybercrime is further complicated by the fact that cybercrime is embedded in networks of *organized* crime. Many of these criminal organizations are physically centered in places outside the reach of U.S. law enforcement such as Russia, China, and North Korea.[32] As this list suggests, some of these criminal organizations are tightly connected with nation-state actors.[33]

---

25. "Steganography" involves hiding information within other information. *See What is Steganography? Definition and Explanation*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/what-is-steganography (last visited Apr. 8, 2023).

26. *See* VLADIMIR KROPOTOV, ROBERT MCARDLE & FYODOR YAROCHKIN, TREND MICRO RSCH., THE HACKER INFRASTRUCTURE AND UNDERGROUND HOSTING: SERVICES USED BY CRIMINALS 17 (2020), https://documents.trendmicro.com/assets/white_papers/wp-the-hacker-infrastructure-and-underground-hosting-services-used-by-criminals.pdf.

27. *See id.*

28. *See id.* at 38–48; *Module 13: Cyber Organized Crime*, UNITED NATIONS OFF. ON DRUGS & CRIME (Apr. 1, 2020), https://www.unodc.org/e4j/zh/cybercrime/module-13/index.html; LILLIAN ABLON, MARTIN C. LIBICKI & ANDREA M. ABLER, RAND CORP., MARKETS FOR CYBERCRIME TOOLS AND STOLEN DATA: HACKERS' BAZAAR 8–15 (2014), https://www.rand.org/pubs/research_reports/RR610.html.

29. *See* Kumar Ritesh, *Who's Buying and Selling Ransomware Kits on the Dark Web*, CYBERCRIME MAG. (Mar. 13, 2021), https://cybersecurityventures.com/whos-buying-and-selling-ransomware-kits-on-the-dark-web/; HP WOLF SEC., THE EVOLUTION OF CYBERCRIME: WHY THE DARK WEB IS SUPERCHARGING THE THREAT LANDSCAPE AND HOW TO FIGHT BACK 4 (2022).

30. HP WOLF SEC., *supra* note 29, at 11; Thomas S. Hyslip, *Cybercrime-as-a-Service Operations*, *in* THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE (Thomas J. Holt & Adam M. Bossler eds., 2020).

31. HP WOLF SEC., *supra* note 29, at 4.

32. *See* Roderic Broadhurst et al., *Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime*, 8 INT'L J. CYBER CRIMINOLOGY 1 (2014). As Broadhurst et al. suggest, it is appropriate to use the term "organized crime" in cyberspace although cybercrime groups take on a variety of forms of organization that challenge traditional definitions of "organized crime." *Id.*

33. *See* C. Todd Lopez, *In Cyber, Differentiating Between State Actors, Criminals Is a Blur*, DOD NEWS (May 14, 2021), https://www.defense.gov/News/News-

Cybercrime is also a hard problem because it is so ubiquitous. No statistics exist on the actual number of individuals who have been affected by data breaches, but a recent RAND Corporation study suggests the number might be nearly half the population in the U.S.[34] The RAND study was based on individual recollection of having received a data breach notification.[35] Of course, not every breach is discovered and reported, meaning the RAND study is underinclusive. Yet other studies suggest that the PII of nearly *every* person in the United States has been exposed in *multiple* data breaches.[36] According to the cybersecurity consultancy Surfshark, there have been nearly 15 billion individual account credentials exposed by breaches since 2004, including nearly 3 billion U.S.-based accounts.[37] This means nearly seven accounts have been breached for each person in the U.S.—in other words, that the average person in the U.S. has had their PII exposed seven different times.[38] The "Have I Been Pwned?" website, which allows anyone to see if their email address or phone number has been compromised in a breach,

Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/ (stating that "[t]he line between nation-state and criminal actors is increasingly blurry as nation-states turn to criminal proxies as a tool of state power, then turn a blind eye to the cyber crime perpetrated by the same malicious actors" (quoting *Operations in Cyberspace and Building Cyber Capabilities Across the Department of Defense: Hearing Before the Subcomm. on Cyber, Innovative Techs., & Info. Sys.*, 117th Cong. 5 (2021) (statement of Mieke Eoyang, Deputy Assistant Sec'y of Def. for Cyber Pol'y, Dep't of Def.))); E.R. Leukfeldt & Thomas J. Holt, *Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline*, 64 INT'L J. OFFENDER THERAPY & COMPAR. CRIMINOLOGY 522, 529 (2019) (finding that none of the cybercrime organizations studies were "loners").

34. LILLIAN ABLON ET AL., RAND CORP., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 9 (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.

35. *Id.*

36. *See* Chad M.S. Steel, *Stolen Identity Valuation and Market Evolution on the Dark Web*, 13 INT'L J. CYBER CRIMINOLOGY 70, 74 (2019).

37. *See Global Data Breach Stats*, SURFSHARK, https://surfshark.com/research/data-breach-monitoring (last visited Apr. 23, 2023). Surfshark's methodology is not fully transparent, and the company acknowledges the data is not likely fully accurate. *See Methodology*, SURFSHARK, https://surfshark.com/research/data-breach-monitoring/methodology (last visited Apr. 23, 2023). Nevertheless, the Surfshark report is broadly consistent with many other data points regarding the massive scale of global cybercrime. *See, e.g.*, Steel, *supra* note 36.

38. *See Global Data Breach Stats*, *supra* note 37.

contains over eleven billion "pwned" accounts.[39] This means there is more than one compromised account for every person on the planet.[40]

As a result of all these factors, cybercrime is an exceptionally difficult problem for law enforcement. The investigation of cybercrime involves "the cooperation of numerous law enforcement agencies—each requiring the capacity and capability to contribute to a multi-agency, transnational investigation."[41] Some authorities estimate that an alleged perpetrator is arrested in only 3 out of every 1,000 criminal cyber incidents (0.3%).[42] The criminal justice system, then, cannot effectively address the harm from cybercrime to the data controller or processor, which is the initial victim, nor to the data subjects whose PII was taken, who are secondary victims.

For the same reasons, cybercrime is a difficult and costly problem for commercial enterprises. A general term such as "careless" might characterize some particularly egregious data breach cases, such as a failure to install routine software patches.[43] In most cases, however, the duty of care is not so clear. Because cybercrime is so pervasive and sophisticated, no compliance standard assumes that any commercial entity could ever perfectly insulate itself from successful attacks.

---

39. *See* ';—HAVE I BEEN PWNED?, https://haveibeenpwned.com (last visited Feb. 2, 2023). "Pwned" is slang derived from video gamers and means "owned"—that is, thoroughly defeated. *See FAQS*, ';—HAVE I BEEN PWNED?, https://haveibeenpwned.com/FAQs (last visited Feb. 2, 2023). The author of this Article searched his personal Gmail address and the two variations of his work email address in "Have I Been Pwned" and found that these three email addresses were disclosed in a total of twenty-three separate breaches, including breaches involving widely used services and products such as Adobe software, Dropbox, and LinkedIn. (Information on file with the author.) Readers may wish to try this exercise, which likely will disclose similar results if the reader has used these or other popular business products or services.

40. The current world population is over 8 billion. *See Current World Population*, WORLDOMETER, https://www.worldometers.info/world-population/ (last visited Apr. 8, 2023). Of course, this does not mean that every person on the planet has been subject to a data breach. There is still a global digital divide, in which nearly half the global population lacks even basic Internet access. *See* Cheng Li, *Worsening Global Digital Divide as the US and China Continue Zero-Sum Competitions*, BROOKINGS (Oct. 11, 2021), https://www.brookings.edu/blog/order-from-chaos/2021/10/11/worsening-global-digital-divide-as-the-us-and-china-continue-zero-sum-competitions/. There is a digital divide even in the U.S. *See* Bhaskar Chakravorti, *How to Close the Digital Divide in the U.S.*, HARV. BUS. REV. (July 20, 2021), https://hbr.org/2021/07/how-to-close-the-digital-divide-in-the-u-s. Data breaches are a first-world problem. *See First World Problem*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/first%20world%20problem (last visited Feb. 2, 2023).

41. Allison Peters & Amy Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, 10 J. NAT'L SEC. L. & POL'Y 487, 488 (2020).

42. Allison Peters & Anisha Hindocha, *US Global Cybercrime Cooperation: A Brief Explainer*, THIRD WAY (June 26, 2020), https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer.

43. *See* Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172 (2021).

All of this means that "cybersecurity" is as much about containing and recovering from intrusions as it is about prevention. The National Institute of Standards and Technology ("NIST") Cybersecurity Framework, for example, is widely considered to be a leading cybersecurity standard.[44] The Framework Core involves familiar problem solving and risk management tools: Identify, Protect, Detect, Respond, and Recover.[45] The Identify Function requires an organization to "[d]evelop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities."[46] Identifying cybersecurity risks, as the Framework suggests, is an organization-wide, continuous effort, not merely a matter of an IT staffer configuring a firewall. "The Protect Function," according to the Framework Core, "supports the ability to limit or contain the impact of a potential cybersecurity event."[47] The language of "limit or contain" reflects the reality that breaches cannot be entirely, absolutely prevented.[48] The Detect, Respond, and Recover Functions further demonstrate that cybersecurity compliance involves the entire organization, not merely the company's IT department. These functions also show that there are multiple decision points in the compliance process about acceptable risk levels and risk management in relation to an organization's mission and resources.[49]

The assumption that every breach is the fault of the data controller or processor, therefore, is inaccurate. The collection and aggregation of consumer PII that powers modern commerce creates risks to data subjects, but those risks are not necessarily actionable "harms" caused by the controller or processor, even when a breach occurs. Any taxonomy of privacy harms resulting from data breaches must drill down into the specifics of contemporary cybercrime.

B. How Cybercrime Complicates the Warren-Brandeis-Prosser-Solove Privacy Taxonomy

In 1960, commenting on Samuel Warren and Louis Brandeis' classic article *The Right to Privacy*, William Prosser identified four types of privacy harms:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.

44. *See Cybersecurity Framework*, NIST, https://www.nist.gov/cyberframework (last visited Feb. 2, 2023).

45. NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 6–7 (2018), https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

46. *Id.* at 7.

47. *Id.*

48. *See id.*

49. *See id.* at 7–8.

2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[50]

Warren and Brandeis wrote their article in 1890, before radio and television. Prosser's elaboration in 1960 predates the commercial Internet age by about four decades, a different geological era in cyber-time.[51] Three of Prosser's four categories involve a *public* use or disclosure of information protected by a right of privacy. Only Prosser's first category lacked any necessary element of public disclosure, and that first category only extended to seclusion, solitude, and private affairs.[52]

In 2006, within the Internet age but only at the dawn of our current epoch of disinformation and cybercrime, Daniel Solove proposed a new taxonomy of privacy that would refine Prosser's work.[53] Solove proposed four categories of "harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion."[54] As Solove notes, the recognition that such activities could be "harmful" in the computer age dates back to sources from the 1970s and 1980s,[55] including Professor Alan Westin's 1967 book *Privacy and Freedom*; a 1973 report of the U.S. Department of Health, Education, and Welfare; the U.S. Privacy Act of 1974; and a set of Organisation for Economic Co-operation and Development ("OECD") guidelines adopted in 1980 that became the basis for the European Union ("EU") Data Protection Directive and later the General Data Protection Regulation ("GDPR").[56]

50. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

51. *See Brief History of the Internet*, INTERNET SOC'Y, https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (last visited Apr. 8, 2023).

52. Prosser, *supra* note 50, at 389.

53. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

54. *Id.* at 489.

55. *See id.*

56. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); U.S. DEP'T HOMELAND SEC., MEMORANDUM NO. 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf; U.S. DEP'T HEALTH, EDUC., & WELFARE, RECORDS, COMPUTER, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (June 30, 1973), https://aspe.hhs.gov/reports/records-computers-rights-citizens; Privacy Act of 1974, 5 U.S.C. § 552a; OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980) https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Solove breaks his four main categories into sub-categories. Under "Information Collection" he lists "Surveillance" and "Interrogation."[57] Here, Solove lists various kinds of concerns, particularly relating to actions taken by the state and actions taken by private parties.[58] As to state action, he cites the basic civil liberties against unreasonable searches and seizures and against self-incrimination embedded in the Fourth and Fifth Amendments.[59] As to private action, he cites the Wiretap Act, the Electronic Communications Privacy Act, and prohibitions against asking certain kinds of questions (*i.e.*, about pregnancy) in an employment context.[60]

Under "Information Processing," Solove includes "Aggregation," "Identification," "Insecurity," "Secondary Use," and "Exclusion."[61] Again, the specific concerns under these sub-headings homogenize state action and private action. The sub-heading "Insecurity" incorporates identity theft.[62] Solove argues that "[v]ictims of identity theft are submerged into a bureaucratic hell where, according to one estimate, they must spend approximately two years and almost 200 hours to decontaminate their [digital] dossier."[63] He blames the growth of identity theft on "[t]he careless use of data by businesses and the government . . . ."[64]

Within "Information Dissemination," Solove lists "Breach of Confidentiality," "Disclosure," "Exposure," "Increased Accessibility," "Blackmail," "Appropriation," and "Distortion."[65] Many of the offenses he cites under these categories fall within the classical Warren-Brandeis-Prosser rubric of privacy harms, such as public disclosure of private facts, commercial misappropriation of a person's name or likeness, and defamation.[66] Under "Invasion," Solove lists "Intrusion" and "Decisional Interference."[67] The examples of "Intrusion" follow Prosser's category of intrusion.[68] Under "Decisional Interference," Solove develops broader arguments about an individual's right to make decisions about sensitive life

57. Solove, *supra* note 53, at 491, 500.

58. *Id.* at 491–505

59. *Id.*

60. *Id.*

61. *Id.* at 505–25.

62. *Id.* at 516–17.

63. *Id.* (citing JANINE BENNER, BETH GIVENS & ED MIERZWINSKI, NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT, pt. II, §§ 1, 4 (2000), https://privacyrights.org/resources/victims-speak-out-identity-theft-survey-identity-theft-victims-and-recommendations-reform [https://web.archive.org/web/20060812141337/https://privacyrights.org/ar/idtheft2000.htm]).

64. *Id.* at 517.

65. *Id.* at 525–52.

66. *See id.* at 530, 546, 549.

67. *Id.* at 552–62.

68. *Id.*

issues, based on the substantive due process cases involving contraception, abortion, and marriage following *Griswold v. Connecticut*.[69]

The Warren-Brandeis-Prosser-Solove taxonomy of "privacy" harms, then, certainly encompasses the actions of hackers who steal PII. Unfortunately, as discussed in Section I.A above, only very rarely will an individual ever obtain a civil remedy directly from a criminal hacker, at least relating to an economic crime, because much of this activity involves international organized crime with connections to nation-states. Individuals in the cybercrime ecosystem involved in a given breach, even if they can be identified, are mostly judgment-proof because they do not have assets subject to attachment in the U.S.[70]

In contrast, almost none of the harms within these rubrics relate to commercial enterprises that lose customer PII when they are also the victims of criminal hackers. The exception is Solove's subcategories of "aggregation" and "insecurity" in the context of "information processing."[71] The commercial victims of criminal hackers collect and retain large amounts of consumer PII, which makes them attractive targets, and exfiltration of PII results from a security breach. In his *Taxonomy of Privacy* and in later work, Solove seems to assume that consumers should have remedies against the targeted commercial enterprises for emotional harms, even absent proof of economic losses.[72]

As I have argued elsewhere, it makes sense for individuals who can demonstrate economic losses to possess a remedy in tort notwithstanding the economic loss doctrine.[73] But this does not necessarily assume strict or

69. 381 U.S. 479 (1965); *see* Solove, *supra* note 53, at 557–62 (first citing *Griswold*, 381 U.S. 479; then citing Eisenstadt v. Baird, 450 U.S. 438 (1972); then citing Roe v. Wade, 410 U.S. 113 (1973); then citing Whalen v. Roe, 429 U.S. 589 (1977); and then citing Lawrence v. Texas, 539 U.S. 558 (2003)). *Roe* was overruled by *Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228 (2022). In his majority opinion in *Dobbs*, Justice Alito noted that if the right to abortion were part of "a broader entrenched right" of privacy, such a right could not be absolute. *Dobbs*, 142 S. Ct. at 2257. Justice Alito suggested that the *Dobbs* decision would not implicate other rights based on a right to privacy based on the concept of substantive due process, such as the right to interracial or same-sex marriage. *Id.* at 2258. Justice Kavanaugh reiterated this conclusion in his concurrence. *Id.* at 2309 (Kavanaugh, J., concurring) (stating "I emphasize what the Court today states: Overruling *Roe* does *not* mean the overruling of those precedents, and does *not* threaten or cast doubt on those precedents"). In a separate concurrence, however, Justice Thomas stated that all of the Court's substantive due process opinions should be reconsidered. *Id.* at 2301–02 (Thomas, J., concurring). The dissent also expressed concern that *Dobbs* casts doubt on other privacy rights. *Id.* at 2338 (Breyer, Sotomayor & Kagan, JJ., dissenting). After *Dobbs*, it is unclear whether or to what extent a right to privacy can still be gleaned from the Constitution's due process clauses.

70. *See, e.g.*, CROWDSTRIKE, *supra* note 24, at 6 (noting that most tracked cyber crime comes from Eastern Europe and Russia).

71. Solove, *supra* note 53, at 491–505.

72. *See generally id.*

73. David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 974 (2016).

absolute liability for every data breach. It is not true that data breaches happen only because the data processor has been careless, nor is it true that most individuals whose PII is compromised in a data breach lose money or time because of the breach. In fact, very often specific items of exfiltrated PII are never used for any kind of fraud that has any direct economic effects on the individual. The next Section explores these complications.

C. How Stolen PII Gets Monetized

The prevalence of cybercrime suggests that it is a profitable activity. So how do data thieves make money? The answers to this question are more complex than might be assumed. This seems counterintuitive. As the Seventh Circuit asked in *Remijas v. Neiman Marcus Group*,[74] "[w]hy 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."[75] The *Remijas* court asked this question in the context of addressing a plaintiff's standing to sue.[76] Other courts have held that, without proof of concrete out-of-pocket harms, plaintiffs lack standing to sue in data breach cases, while yet others agree with *Remijas*.[77] The Article III standing question has become even more muddied after the Supreme Court's 2021 holding in *TransUnion LLC v. Ramirez*[78] restricting standing in certain cases under the Fair Credit Reporting Act.[79] And even some courts that have found Article III standing have subsequently dismissed the plaintiffs' tort claims on the merits as a matter of law for failure to assert ascertainable damages.[80]

74. 794 F.3d 688 (7th Cir. 2015).

75. *Id.* at 693.

76. *Id.*

77. *See* David W. Opderbeck, *Current Developments in Data Breach Litigation: Article III Standing After* Clapper, 67 S.C. L. REV. 599, 607 (2016).

78. 141 S. Ct. 2190 (2021).

79. Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; *Ramirez*, 141 S. Ct. at 2200, 2214; James Dempsey, *US Courts Mixed on Letting Data Breach Suits Go Forward*, INT'L ASS'N OF PRIV. PROS. (May 9, 2022), https://iapp.org/news/a/u-s-courts-mixed-on-letting-data-breach-suits-go-forward/#:~:text=The%20Supreme%20Court%20has%20been,particularized%2C%20and%20actual%20or%20imminent; James Dempsey, *Chapter 4A Standing After* TransUnion, CYBERSECURITY L. FUNDAMENTALS (Feb. 22, 2023), https://cybersecuritylawfundamentals.com/chapter-4a.

80. *See, e.g.*, Stollenwerk v. Tri-West Health Care All., 254 F. App'x 664 (9th Cir. 2007); Ruiz v. GAP, Inc., 622 F. Supp. 2d 908 (N.D. Cal. 2009); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007); Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008); Adkins v. Facebook, Inc., 424 F. Supp. 3d 686 (N.D. Cal. 2019); Gardner v. Health Net, Inc., No. CV 10-2140 PA (CWx), 2010 WL 11597979, at *1 (C.D. Cal. Aug. 12, 2010); Holmes v. Countrywide Fin. Corp., No. 5:08-CV-00205-R, 2012 WL 2873892, at *1 (W.D. Ky. July 12, 2012); Krottner v. Starbucks Corp., No. C09-0216RAJ, 2009 WL 7382290, at *1 (W.D. Wash. Aug. 14, 2009); Randolph v. ING Life Ins. and Annuity Co., 973 A.2d 702 (D.C. 2009); Hammond v. Bank

The confusion in the case law, both relating to Article III standing and to tort claims on the merits, stems in significant part from a lack of detailed attention to what actually happens to exfiltrated consumer PII. As noted in Section I.A above, the average American's PII has been exposed in multiple different data breaches. No data even remotely suggests that there have been billions of instances of unreimbursed out-of-pocket expenses to American individuals resulting from data breaches.[81] It seems that most of the time breached PII falls into a black hole and never gets monetized or reused.[82] In some cases, individuals whose PII is compromised in a data breach suffer tangible pecuniary harms, in other cases not.[83] In some cases, such individuals may suffer a reasonable amount of fear or anxiety, in other cases not—and even if *some* fear or anxiety is warranted, the *degree* of fear and anxiety may in some cases be reasonably substantial, in other cases not.[84] A related problem for any general discussion of data breach harms is that the degree and nature of any such harm may argue in favor of different kinds of legal responses—particularly, through private law remedies in tort or through regulatory fines and penalties.[85]

A complicating factor is that the nature and profitability of cybercrime has shifted in recent years. Ransomware has become increasingly prevalent.[86] In a ransomware attack, the cybercriminal infiltrates a target system and encrypts critical data. The data is decrypted and released to the data processor only after the payment of a ransom.[87] Most ransomware attacks do not

of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *1 (S.D.N.Y. June 25, 2010). Many such cases arise from physical device thefts or losses rather than malware-based system hacks. These include stolen server computers, *Stollenwerk*, 254 F. App'x at 665, stolen or misplaced laptops, *Ruiz*, 622 F. Supp. 2d at 910; *Caudle*, 580 F. Supp. 2d at 276; *Krottner*, 2009 WL 7382290, at *1, stolen or misplaced unencrypted hard drives or backup tapes, *Gardner*, 2010 WL 11597979, at *1; *Hammond*, 2010 WL 2643307, at *2, and insider theft, *Holmes*, 2012 WL 2873892, at *1. The distinction is not always clear in the cases, but the question of causation seems far more attenuated in device theft or loss cases than in malware-based system breaches. A device that is merely misplaced might end up in a dusty corner or in a landfill and may never be accessed by anyone. A single stolen drive or device looks like a crime of opportunity, which might be more about the device itself than the data it contains.

81. *See supra* notes 32–38 and accompanying text.

82. *See supra* notes 32–38 and accompanying text.

83. *See supra* notes 32–38 and accompanying text.

84. *See supra* notes 32–38 and accompanying text.

85. *See supra* notes 32–38 and accompanying text.

86. *See* CROWDSTRIKE, *supra* note 24, at 11; HP WOLF SEC., *supra* note 29, at 9.

87. *See Stop Ransomware*, U.S. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware (last visited Mar. 5, 2023); Sean Michael Kerner, *Ransomware Trends, Statistics, and Facts in 2023*, TECHTARGET, https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#:~:text=Ransomware%20statistics%20for%202021%20and%202022&text=Ransomware%20affected%2066%25%20of%20organizations,about%20ransomware%20attacks%20in%202021 (last visited May 11, 2023) (noting that "ransomware attacks surged dramatically in 2022"); JOHN

involve exfiltration of consumer PII because the point of the attack is not to use or resell the data.[88] In fact, the rise of ransomware is to some extent the result of saturation in markets for consumer PII.[89] There simply is more money and easier money in ransomware.

Nevertheless, "traditional" data breaches in what data is exfiltrated rather than only ransomed still occur regularly.[90] There seems to be no reason for a system breach other than to profit from the stolen information, so the harm should show up *somewhere*. In fact, if we more precisely categorize non-ransomware data breaches, we can see that the vast majority of harm is systemic—a cost to the consumer credit system that attenuates the value of the credit benefit—rather than individualized. The categories include (1) credit card fraud, which can involve card present ("CP") or card not present ("CNP") transactions; (2) resale; (3) true identity theft; (4) synthetic identity fraud; (5) social engineering campaigns; (6) market manipulation; (7) trade secret theft; and (8) state surveillance. These are discussed below.

1. Payment Card Fraud

Payment card fraud was one of the earliest kinds of commercial cybercrime.[91] Stolen card numbers are bundled and sold on the dark web through well-established markets. At some point, a purchaser of stolen card information can try to monetize it by making fraudulent purchases of retail goods, services, or gift cards.[92] The person or group making these retail purchases often is not the original data thief. In some cases, data theft rings have used money mules to obtain cash-like tokens or to purchase virtual currencies using stolen card numbers.[93] Occasionally, retail purchasers using

---

SAKELLARIADIS, ATL. COUNCIL, BEHIND THE RISE OF RANSOMWARE 2 (2022), https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Behind_the_rise_of_ransomware.pdf (noting that ransomware "has grown exponentially in recent years, whether measured in the volume of attacks, the money flowing to criminals, or the harms inflicted on society"). As Sakallariadis also notes, "business interruption losses—and not the threat of proprietary data loss or brand damage—represent the most consequential pain point for most victims." *Id.* at 7.

88. *See* SAKELLARIADIS, *supra* note 87, at 7.

89. *See id.*

90. *See generally* CROWDSTRIKE, *supra* note 24; HP WOLF SEC., *supra* note 29; FBI, INTERNET CRIME REPORT 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

91. For a narrative account of payment card fraud, see KEVIN POULSEN, KINGPIN: HOW ONE HACKER TOOK OVER THE BILLION-DOLLAR CYBERCRIME UNDERGROUND (Crown Reprint ed. 2012).

92. *See, e.g.*, *Most Common Purchases with Stolen Credit Card Information*, TRANSUNION (July 6, 2021), https://www.transunion.com/blog/identity-protection/most-common-purchases-with-stolen-credit-card-information.

93. *See What is a Money Mule Scam?*, CRYPTOPEDIA (Jan. 31, 2022), https://www.gemini.com/en-US/cryptopedia/what-is-a-money-mule-scam-crypto#section-how-money-mule-schemes-move-money; *Money Mule Initiative*, U.S. DEP'T OF JUST. (Mar. 10, 2023),

fraudulent payment cards will acquire goods meant for their own consumption.[94] More often, the end purchaser (sometimes called a "stuffer") acquires high-value fungible items such as expensive jewelry and launders delivery of the product through reshipment scams.[95] These goods must be fenced through resale in black markets or on recognized sites such as eBay to be converted to cash.[96]

Credit card fraud can be subdivided into CP and CNP transactions. For a CP transaction, the card number can be encoded onto the magnetic strip of a counterfeit physical card using a fake name and then used to buy goods at a physical retail location that does not yet use chip and pin or tap cards, including many U.S. gas stations.[97] CNP transactions, in contrast, include most online purchases. In most cases, a card cannot be used for a CNP transaction unless the name, address, and CCV number entered into the merchant's website match those assigned to the card number in the payment processor's database.[98] The thief or fence therefore must obtain and use not only the card number, but also the cardholder's name and address.

Sometimes a single tranche of stolen data will provide the full package of information necessary to engage in a CNP transaction or other form of identity theft—a collection known as a "fullz."[99] More often, information from different sources must be combined to create a fullz. Cyber thieves may combine PII from different dark web sources with PII openly available on the

https://www.justice.gov/civil/consumer-protection-branch/money-mule-initiative#:~:text=Money%20mules%20are%20people%20who,serious%20consequences%E2%80%94including%20criminal%20charges; Brian Krebs, *'Money Mule' Gangs Turn to Bitcoin ATMs*, KREBSONSECURITY (Sept. 29, 2016), https://krebsonsecurity.com/2016/09/money-mule-gangs-turn-to-bitcoin-atms/.

94. *See Most Common Purchases with Stolen Credit Card Information*, *supra* note 92. Nearly everyone has a story about dealing with fraudulent charges on a personal credit card. In the author's case, this has involved a fraudulent charge for an online dating service. The author has been happily married for thirty years and was in the awkward position of assuring his spouse that a data thief bought the Match.com subscription. On another occasion, a data thief used the author's card to purchase a pizza and rent some movies. Presumably these were small-scale operators—in one case, almost certainly a checkout clerk at a less than upscale hotel.

95. *See With Stolen Cards, Fraudsters Shop to Drop*, KREBSONSECURITY (Sept. 28, 2015), https://krebsonsecurity.com/2015/09/with-stolen-cards-fraudsters-shop-to-drop/.

96. *See, e.g.*, POULSEN, *supra* note 91; Sara Peters, *How to Monetize Stolen Payment Card Data*, DARKREADING (Apr. 13, 2016), https://www.darkreading.com/threat-intelligence/how-to-monetize-stolen-payment-card-data.

97. *See* Paul Bischoff, *Dark Web Prices for Stolen PayPal Accounts Up, Credit Cards Down: Report*, COMPARITECH (Sept. 8, 2021), https://www.comparitech.com/blog/vpn-privacy/dark-web-prices/ (discussing the distinction between physical "cloned" cards and online purchases).

98. *See Card Present vs. Card Not Present Fraud (CP vs. CNP)*, NAT'L MERCHS. ASS'N, https://www.nationalmerchants.com/cp-vs-cnp-fraud-card-present-vs-card-not-present/ (last visited Apr. 9, 2023).

99. *See* Robert Lemos, *All About Your 'Fullz' and How Hackers Turn Your Personal Data into Dollars*, PCWORLD (June 2, 2016, 4:30 AM), https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html.

surface web through social media sites and other sources where users have voluntarily posted this information.[100] In other words, exfiltrated PII such as payment card numbers typically is one component of a larger data mining operation that involves both illicit and licit sources.

On one hand, the out-of-pocket harm from stolen payment card information seems obvious: Someone can use the card to make a fraudulent charge. But under U.S. law, an issuing bank must reimburse a cardholder for any fraudulent charges in excess of $50, while the agreements that govern all the major card brands require full reimbursement to the cardholder for fraudulent charges.[101] The consumer suffers no out-of-pocket loss for the repayment of fraudulent charges.[102]

Even with this reimbursement requirement, some consumers might suffer some out-of-pocket harm for lost opportunities or lost time. During the period between the fraudulent use of the credit card and the detection of such use, the consumer may suffer loss of access to some or all of their credit benefit because no consumer has an infinite credit line. In many cases, however, the issuing bank's fraud detection systems flag the suspect transaction before impinging on any desired access to the credit line by the consumer.[103] Even if the consumer suffers some temporary contraction of their credit benefit, once the fraud is detected, the full benefit is restored. Perhaps in some cases a consumer loses access to a good or service subject to limited availability or the benefit of a temporary sale price or dip in market price because a full credit line was not immediately available. Or, maybe, the customer faces the classic romantic comedy dilemma if fraud exhausts the credit line: He or she takes out the card to pay for dinner with a date, the card is declined, and the date must be asked to pony up for the bill.[104] Such cases would seem to be relatively rare.

The cardholder may also suffer some loss of time correcting fraudulent transactions. In many cases, however, the consumer is notified of suspicious transactions by the issuing bank's screening procedures.[105] If the consumer does notice something suspicious, most issuing banks now employ

100. *See* Yizhi Liu et al., *Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web*, 2020 IEEE INT'L CONF. ON INTEL. & SEC. INFORMATICS, Nov. 9, 2020, at 1, https://ieeexplore.ieee.org/document/9280540.

101. 15 U.S.C. § 1666i(a); *see* Opderbeck, *supra* note 73, at 942.

102. *See* Opderbeck, *supra* note 73, at 942.

103. *Fraud Protection All Day, Every Day*, CHASE, https://www.chase.com/digital/fraud-security (last visited Mar. 5, 2023); *Capital One Fraud Protection*, CAPITAL ONE, https://www.capitalone.com/bank/security-fraud-protection/ (last visited Mar. 5, 2023).

104. *See Credit Card Destruction*, TVTROPES, https://tvtropes.org/pmwiki/pmwiki.php/Main/CreditCardDestruction (last visited Mar. 5, 2023).

105. *See, e.g.*, *Visa Dispute Monitoring and Visa Fraud Monitoring Programs (VDMP & VFMP)*, CHARGEBACK GURUS (Dec. 31, 2021), https://www.chargebackgurus.com/blog/visa-dispute-and-fraud-monitoring-programs-vdmp-vfmp.

straightforward web or telephone-based reporting mechanisms.[106] It should be a rare case in which a consumer loses any significant amount of time dealing with fraudulent payment card charges.

The agreements that connect the issuing bank, acquiring bank, merchant, and card brand further contain policies and procedures for adjusting these charges among the banks and merchant if the breach related to a failure to implement contractually agreed-upon security measures.[107] The real harm from most payment card breaches, then, is not to any individual consumer whose payment card information has been compromised. The real harm is spread throughout the payment card networks and affects the global value of the credit benefit.

A functioning credit system results in a substantial "credit benefit" to the economy.[108] As William Roberds and Stacey Schreft noted in 2009, if the credit benefit from payment cards used by U.S. residents amounted to only 5 percent of the total value of transactions ($3 trillion in that year), the total value of the credit benefit would be $150 billion.[109] Using Roberds and Schreft's estimate today for Mastercard and Visa purchases alone in the United States would yield a credit benefit of nearly $370 billion—about $1,121 for each person or $1,797 per cardholder.[110]

This is significant for our discussion of data breach harms: Consumers have disclosed their PII to the banks in exchange for their share of the credit

106. *See, e.g.*, *Capital One Fraud Protection*, *supra* note 103.

107. *See* Opderbeck, *supra* note 73, at 941.

108. Roberds & Schreft, *supra* note 16, at 23–24.

109. *Id.* at 24. The total value of such transactions in 2006, when Roberds and Schreft wrote their paper, was $3 trillion. *Id.* Roberds and Schreft concluded that a conservative $150 billion credit benefit would outweigh the total cost of identity theft. *Id.* at 24. That conclusion was based on the Federal Trade Commission's ("FTC") estimation of the cost to consumers of identity fraud along with a study by Schreft suggesting that consumers lost $61 billion to identity theft in 2006. *See id.* at 22.

110. According to *Nilson Report*, the combined volume of Mastercard and Visa purchases in 2021 was $7.387 trillion. *Mastercard and Visa in the U.S.—2021*, NILSON REP. (Feb. 15, 2022), https://nilsonreport.com/mention/1556/1link/. Five percent of 7.387 trillion is 369.35 billion. The total U.S. population is approximately 330 million people. *See Population Estimates, July 1 2021, (V2021)*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045221 (last visited Apr. 24, 2023). About 78% (or 257,400,000 people) of the U.S. population is over age 18. *See id.* About 80% of American adults hold at least one payment card. *See* Ivana Pino, *Credit Card Ownership and Usage Statistics*, BANKRATE (Feb. 23, 2022), https://www.bankrate.com/finance/credit-cards/credit-card-ownership-usage-statistics. Therefore, about 205,920,000 people in the U.S. hold at least one payment card. In fact, most people hold more than one payment card. Jamie Gonzalez-Garcia & Tamara E. Holmes, *Credit Card Ownership Statistics*, CREDITCARDS.COM (May 24, 2021), https://www.creditcards.com/statistics/ownership-statistics/#sources; Pino, *supra*. The average American's credit card debt is over $5,200. *See* Chris Horymski, *Average Credit Scores Hit New High, While Debt Balances Rise*, EXPERIAN (Feb. 24, 2023), https://www.experian.com/blogs/ask-experian/consumer-credit-review/. This may suggest, perhaps not surprisingly, that the average American consumer is over-leveraged in relation to their share of the credit benefit.

benefit. If the disclosure of PII represents some loss of personal autonomy, then consumers value that measure of autonomy at least equal to the credit benefit they receive from the payment card system.[111] In exchange for surrendering that measure of autonomy, consumers receive a token—a credit card number—that allows them to exercise their allotted measure of credit. The card brands, banks, merchants, and consumers know that some amount of fraud is inevitable, and this inevitability is built into credit terms and rates.

2. Resale

The nature of CNP transactions illuminate the second major reason why thieves steal PII apart from payment card numbers: To sell it on the dark web so that other users can combine it with card numbers and information to conduct payment card fraud. Dark web markets exist for pilfered PII along with cybercrime tools and services.[112] One tranche of stolen PII might contain John Doe's name, card number, and PIN, while another tranche may contain Doe's name and address. These individual tranches are not as valuable as an assembled Fullz.[113] Individual pieces of stolen data are often combined with other stolen or fabricated information, including even fake identification photos, to create a Fullz.[114] This dynamic helps explain why individuals whose PII is exposed as part of a breach may never experience a fraudulent payment card transaction. If only parts of their PII were exposed in a single breach, the exposure may not support CNP transactions.

Surveys of pricing for PII on the dark web vary. A credit card number alone fetches only about $5–$20 on the dark web.[115] In contrast, a Fullz sells for about $30–$120.[116] Some studies suggested the market price for a Fullz

111. See discussion in Roberds & Shreft, *supra* note 16.

112. *See, e.g.*, Tyler Moore, Richard Clayton & Ross Anderson, *The Economics of Online Crime*, 23 J. ECON. PERSPS. 3, 3–4 (2009); ABLON ET AL., *supra* note 28.

113. *See The Price Cybercriminals Charge for Stolen Data*, TRUSTWAVE: SPIDERLABS BLOG (Aug. 3, 2022), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/.

114. *Id.*

115. *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; *cf.* Patricia Ruffio, *Dark Web Price Index 2022*, PRIV. AFFS. (Apr. 4, 2023), https://www.privacyaffairs.com/dark-web-price-index-2022/.

116. Stack, *supra* note 115; *see also Dark Web Links to Access Darknet Markets*, DARK WEB LINKS, https://www.thedarkweblinks.com/page/4/ (last visited Mar. 5, 2022); *A Look Into the Pricing of Stolen Identities for Sale on Dark Web*, SECURITY (Jan. 22, 2021), https://www.securitymagazine.com/articles/94405-a-look-into-the-pricing-of-stolen-identities-for-sale-on-dark-web; Bischoff, *supra* note 97; Stack, *supra* note 115; Per Håkon Meland, Yara Fareed Fahmy Bayoumy & Guttorom Sindre, *The Ransomware-as-a-Service Economy Within the Darknet*, 92 COMPUTS. & SEC. 101,762, 101,763–64 (2020) https://www.sciencedirect.com/science/article/pii/S0167404820300468; EUROPOL, INTERNET

dropped precipitously from a high of $150 in 2007 to a high of $1.50 in 2016—an astonishing 99% decrease apparently resulting from market saturation.[117] A 2019 study found that a Fullz could be purchased for as low as $0.004 per record, although prices varied widely depending on value-added services and other factors.[118] According to the author of that study, "[b]ecause most adults in the United States have had their identities stolen and sold multiple times based on large scale breaches, the value of 'zero day' or 'first sale' identities has become negligible."[119] The complexity of these markets is a key reason why specific harms are difficult to connect with any specific data breach.

3. True Identity Theft

True identity theft is the assumption of the victim's identity as verified by PII, such as Social Security or driver's license numbers. [120] A criminal actor can use stolen PII in true identity theft to open new lines of credit in the victim's name, including new credit cards, personal loans, business loans, or mortgages. Criminal actors also employ true identity theft to file for tax refunds, welfare, insurance, or pension benefits in the victim's name.[121]

Usually, the victim detects this kind of fraud expeditiously when they receive payment notices for credit lines they did not obtain, statements for private insurance or government benefits they did not receive, or contact from a financial institution, company, or government agency.[122] In the case of private credit and insurance, the relationship between the lender and consumer is contractual, so the victim, who did not actually assent to the

ORGANISED CRIME THREAT ASSESSMENT (2020), https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

117. Steel, *supra* note 36, at 76.

118. *Id.* at 79.

119. *Id.*

120. *See Warning Signs of Identity Theft*, FTC, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Apr. 24, 2023); ERIKA HARRELL, U.S. DEP'T OF JUST., BUREAU OF JUST. STAT., VICTIMS OF IDENTITY THEFT, 2018, at 2, (2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

121. *See Warning Signs of Identity Theft*, *supra* note 120.

122. *See* HARRELL, *supra* note 120, at 1. According to the Bureau of Justice Statistics ("BJS") report, "[a]mong victims who resolved the financial and credit problems associated with their identity theft, more than half (55%) did so in 1 day or less." *Id.* The BJS report further notes that "[a]mong victims who experienced misuse of an existing account, 46% discovered the incident when a financial institution contacted them about suspicious activity on their account, while 21% noticed fraudulent charges on their account." *Id.* at 7. According to the BJS, 28% of victims discovered the incident "by notification from a company or agency that was not a financial institution," 15% received a bill or were contacted about an unpaid bill, and 12% discovered the incident "when they had problems with applying for a loan, applying for governmental benefits, or filing income tax returns." *Id.*

terms, will not be liable to repay the loans. This provides a market incentive for commercial lenders and insurers to employ fraud detection systems before extending substantial lines of credit. In the case of government benefits, similarly, the individual legitimately entitled to benefits does not lose that entitlement because of the fraudster's actions, and the government likewise has an incentive to employ fraud detection systems and to prosecute offenders. The largest systemic costs of true identity theft, then, fall initially on the financial services firms and on the government, which lose money to fraudsters and spend money on fraud detection and prosecution. These costs, of course, are passed on to consumers through higher fees and interest rates and to the entire tax base through depletion of government funds.

It is true, however, that the mechanisms for unwinding true identity theft are not as well established as those for existing credit card fraud. A small percentage of victims must spend more time and money, including for legal counsel and accountants, to cancel transactions and correct the record.[123] Further, unlike a credit card, a Social Security number cannot simply be canceled, so the individual may face repeated incidents of credit identity fraud.[124] Moreover, in addition to the fraudulent loans themselves, the victim's credit score could be adversely affected, which takes additional time and expense to fix, and which could result in opportunity costs to the victim.[125] It seems clear, then, that an individual can face tangible costs resulting from true identity theft.

But for all the attention paid to it, this kind of true identity theft resulting from a large-scale data breach is rare.[126] According to the most recent *Victims of Identity Theft* report from the U.S. Bureau of Justice Statistics, less than one percent of victims who reported identity theft experienced the misuse of their PII for the purpose of obtaining medical care, a job, or governmental benefits.[127] In contrast, ninety percent of victims experienced fraud or attempted fraud involving an existing account, such as a payment card or bank account.[128] In contrast to payment card fraud, it takes effort and sophistication to use a stolen Social Security number to file for government benefits or apply for credit, and these kinds of transactions are distinctive and

123. *See id.* at 10 (noting that about two percent of all victims reported credit problems, and two percent reported "significant problems with family members or friends").

124. *See* Louis DeNicola, *Does Credit Card Fraud Affect Your Credit?*, EXPERIAN (Aug. 21, 2020), https://www.experian.com/blogs/ask-experian/does-credit-card-fraud-affect-your-credit/#:~:text=Credit%20card%20fraud%20can%20impact,no%20longer%20impact%20your%20credit.

125. *See id.*

126. *See* HARRELL, *supra* note 120, at 1.

127. *Id.*

128. *Id.*

easy to trace, making the risk of getting caught relatively high. For most cybercriminals, the potential reward is not worth the effort and risk.

This is not to suggest financial services firms are free of any legal duties relating to true identity fraud. In the rare case where a consumer really is stuck in a "bureaucratic hell," there could be a remedy for out-of-pocket losses if breach and causation can be established. And the burden of detecting and remediating new account fraud should rest squarely on the shoulders of the card brands and banks. They are best positioned to innovate effective detection and remediation systems, and which already have strong market incentives to implement such systems. As discussed in Section III.D below, this is already the case under U.S. law, although the regulations could be improved in important ways. As further discussed in Section III.D, the problem is exacerbated in the United States by our antiquated nine-digit Social Security number system, which needs to be updated for the digital age. These kinds of systemic measures differ from individual private actions for dignitary, emotional, or prophylactic remedies.

4. Synthetic Identity Fraud

Another possibility is that PII can be used for "synthetic" identity fraud. In synthetic identity fraud, authentic information from different people is mixed with fabricated information to create a fictitious composite, which can be employed to obtain credit or hide the true identities of persons engaged in various criminal activities.[129]

As with true identity theft, synthetic identity fraud imposes systemic costs throughout the financial system and across the tax base, and there are strong market incentives for financial services firms to detect and mitigate synthetic identity fraud. No lender wants to extend credit to a fictitious person with fictitious assets. But an individual whose PII is used to create a synthetic composite almost certainly will never know what has happened and will not usually experience any adverse financial claims or effects.

5. Embarrassment, Blackmail, Stalking, Catfishing

Cyber blackmail, cyber stalking, sextortion, doxing, catfishing, and related forms of online embarrassment, fraud, and harassment are enormous problems.[130] Most instances of this conduct arise between former romantic

129. *See* Louis DeNicola, *What is Synthetic ID Fraud?*, EXPERIAN (Aug. 17, 2021), https://www.experian.com/blogs/ask-experian/what-is-synthetic-identity-fraud-theft/; Elaine S. Povich, *Thieves Hit on a New Scam: Synthetic Identity Fraud*, PEW: STATELINE (Apr. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/04/07/thieves-hit-on-a-new-scam-synthetic-identity-fraud.

130. *See, e.g.*, *Cyberstalking: Two Federal Cases Illustrate the Consequences of Sextortion*, FBI (Oct. 30, 2018), https://www.fbi.gov/news/stories/sentences-in-separate-cyberstalking-cases-

partners, friends, or acquaintances, or over social media networks through vectors that do not involve data breaches.[131] Sometimes information derived from breached PII is used to establish a mark for fraudulent schemes, and sometimes, as in the Ashley Madison and Sony cases, PII from a data breach is disclosed to embarrass the individual victims and to pressure the commercial victim.[132] In either case, the person disclosing the information could be liable under one of the traditional common law categories of privacy harm: public disclosure of private facts.[133]

6. Social Engineering Campaigns and Ransomware

Stolen PII could also be used to facilitate social engineering campaigns that provide opportunities for further data breaches or for ransomware. A dark web portfolio on a corporate executive gleaned from stolen PII, for example, could be used to build a convincing spear phishing campaign. It is fairly easy, however, to construct social engineering campaigns from publicly available information on corporate websites and news sources, so the use of PII from data breaches to build the initial campaign seems rare.[134]

If an individual's PII is used to facilitate a ransomware attack on that person's personal computer or to a business owned by that individual, the harm is obvious. But, if an individual's PII is used to facilitate a social engineering or ransomware attack on another entity, the harm to the

103018; *Ranking Needs for Fighting Digital Abuse: Sextortion, Swatting, Doxing, Cyberstalking and Nonconsensual Pornography*, NAT'L INST. OF JUST. (Nov. 20, 2020), https://nij.ojp.gov/topics/articles/ranking-needs-fighting-digital-abuse-sextortion-swatting-doxing-cyberstalking (noting that "[s]tudies indicate that between 18% and 37% of American adults have experienced severe harassment online").

131. *See, e.g.*, *Teen Cyberbulling Context Assessed in the Context of Social Networks*, NAT'L INST. OF JUST. (July 20, 2020), https://nij.ojp.gov/topics/articles/teen-cyberbullying-content-assessed-context-social-networks.

132. *See* Zak Doffman, *Ashley Madison Hack Returns To 'Haunt' Its Victims: 32 Million Users Now Watch And Wait*, FORBES (Feb. 1, 2020, 7:06 AM), https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait; Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/; Brian Barrett, *DoJ Charges North Korean Hacker for Sony, WannaCry, and More*, WIRED (Sept. 6, 2018, 3:12 PM), https://www.wired.com/story/doj-north-korea-hacker-sony-wannacry-complaint/.

133. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977) ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

134. *See, e.g.*, Jason Firch, *How to Create an Email Phishing Campaign in 8 Steps*, PURPLESEC (Sept. 13, 2022) https://purplesec.us/phishing-campaign/; Gavin Debetaz, *Modern Spear Phishing Emails*, TRACESECURITY (Oct. 8, 2021), https://www.tracesecurity.com/blog/articles/crafting-a-modern-spear-phishing-email (noting that "[m]any companies make [reconnaissance] easy for an attacker by making their information easily accessible on their company website").

individual is less obvious. For example, if John Doe is a Vice President at Acme Bank, and Doe's PII is used to construct a convincing phishing campaign that results in a ransomware attack on Acme, Doe does not suffer any immediate pecuniary losses. Perhaps Doe will suffer some losses if the business flounders because of the attack, or if Doe's reputation suffers because his name is associated with the problem, but these harms seem remote. Some of Acme's customers may suffer losses if their accounts are inaccessible, but this kind of business interruption injury is not really a privacy harm. Business interruption may occur for various reasons that can be covered by contracts and insurance.[135]

7. Market Manipulation

Some very sophisticated cyber criminals use stolen information to manipulate public equity markets. The most basic form of cyber-enabled market manipulation is the theft of insider information about business or market circumstances likely to affect share prices and the use of that information to time market trades.[136] Another form of market manipulation involves identity theft in which the thief takes over a victim's brokerage account to implement a pump-and-dump scheme. The thief uses available funds to purchase large quantities of shares in a penny stock, which attracts market attention that further boosts the share price. At a certain point, the thief dumps the stock and cashes out the proceeds, both draining the user's account and crashing the market for the stock.[137]

Individuals whose accounts are breached may suffer out of pocket losses if they are unable to recover depleted investment funds. Since these are discrete accounts, it is easy to connect these losses with a specific breach. Unlike deposit bank accounts, private brokerage accounts are not federally insured, and unlike payment cards, there are no standard intra-industry contracts that adjust for cybersecurity risks. Some leading private brokerage firms contractually agree to cover client losses due to unauthorized activity.[138]

135. *See generally What is Business Interruption Insurance?*, HARTFORD, https://www.thehartford.com/business-insurance/business-interruption-insurance (last visited Apr. 10, 2023); *What is Business Interruption Insurance?*, ALLSTATE (Dec. 1, 2021), https://www.allstate.com/resources/business-insurance/business-interruption-coverage.

136. For a good overview of various kinds of market manipulation, see TOM SWIERS, SEC. & EXCH. COMM'N, MARKET MANIPULATION (2020), https://www.sec.gov/files/Market%20Manipulations%20and%20Case%20Studies.pdf; Tom C.W. Lin, *The New Market Manipulation*, 66 EMORY L.J. 1253, 1256 (2017).

137. Lin, *supra* note 136, at 1285.

138. *See, e.g.*, *Security Guarantee*, CHARLES SCHWAB https://www.schwab.com/schwabsafe/security-guarantee (last visited Mar. 6, 2023).

8. Trade Secret Theft

Trade secret theft is a major motivation for commercial cybercrime.[139] Both private and nation-state actors engage in commercial trade secret theft. It is possible that some PII could get exfiltrated as part of a trade secret theft, but ordinarily this would involve only ancillary information such as the names of employees who worked on a proprietary technology.[140]

9. State Surveillance

A final possibility is that PII is being used by nation-state actors for surveillance, propaganda, and espionage.[141] At first blush, this seems far-fetched. Why would Russia or China care about the online profile of someone like me, a mild-mannered, late middle-aged law professor with no obvious connections to U.S. intelligence sources? In China's case, the reason could be that the data is being used to train and experiment with artificial intelligence systems intended to predict and influence opinion or market trends.[142] In Russia's case, the reason could be that the data is being used to develop disinformation campaigns, such as those used to interfere with our last two presidential elections.[143] Nation-state actors also actively seek to discern the identities of people who work in vulnerable infrastructure

139. *See, e.g.*, U.S. DEP'T OF JUST., DEPARTMENT OF JUSTICE REPORT TO CONGRESS PURSUANT TO THE DEFEND TRADE SECRETS ACT (2019), https://www.justice.gov/criminal-ccips/page/file/1101901/download.

140. For data on trade secret theft, see SYEDAH AILIA HAIDER ET AL., ECONOMIST, OPEN SECRETS? GUARDING VALUE IN THE INTANGIBLE ECONOMY (2021), https://cms.law/en/media/international/images/publications/exclusive-images/open-secrets/open-secrets-guarding-value-in-the-intangible-economy?v=2. In one well-publicized case, the U.S. Department of Justice indicted the Chinese telecommunications company Huawei for allegedly stealing trade secrets from T-Mobile, including information relating to a robot named "Tappy." *See* Indictment, United States v. Huawei Device Co., No. 2:19-cr-00010 (W.D. Wash. filed Jan. 16, 2019), https://www.justice.gov/opa/press-release/file/1124996/download. Huawei's motion to dismiss the Indictment is scheduled to be argued on April 16, 2024, and the case is presently scheduled for trial in October 2024. *See* Fifth Amended Case Schedule, *Huawei*, No. 2:19-cr-00010, 2023 U.S. Dist. Ct. Motions LEXIS 15392.

141. *See, e.g.*, *The Nation State Actor: Cyber Threats, Methods and Motivations*, BAE SYS., https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor (last visited Mar. 6, 2023); *Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited Mar. 6, 2023) (citing numerous incidents of state actor attacks).

142. *See* DAKOTA CARY, GEO. UNIV. CTR. FOR SEC. & EMERGING TECH., ACADEMICS, AI, AND APTS: HOW SIX ADVANCED PERSISTENT THREAT-CONNECTED CHINESE UNIVERSITIES ARE ADVANCING AI RESEARCH 1, 9 (2021), https://cset.georgetown.edu/publication/academics-ai-and-apts/; WM. C. HANNAS ET AL., GEO. UNIV. CTR. FOR SEC. AND EMERGING TECH., CHINA'S ADVANCED AI RESEARCH: MONITORING CHINA'S PATHS TO "GENERAL" ARTIFICIAL INTELLIGENCE 22 (2022), https://cset.georgetown.edu/publication/chinas-advanced-ai-research/.

143. Young Mie Kim, *New Evidence Shows How Russia's Election Interference Has Gotten More Brazen*, BRENNAN CTR. FOR JUST. (Mar. 5, 2020), https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more.

industries, such as banking, public utilities, health care, or military contractors. This information could facilitate blackmail, extortion, or social engineering campaigns that open backdoors for strategic and weaponized malware. These are very real, and very concerning, possibilities. However, unless an individual is subject to blackmail or extortion—a rare occurrence—the harm here is systemic and not personal.

10. Summary

The discussion above shows that the motivations for exfiltration of PII from commercial sources vary and that, in most data breach events, individual consumers are unlikely to suffer direct unreimbursed economic costs. True identity theft is rare in relation to the volume of stolen PII, and the circumstances in which an individual must expend significant time and money to rectify identity theft are rarer still. The overwhelming economic harms from data breaches, then, are systemic, not personalized. If individuals are entitled to personal remedies from data processors who lose PII through a breach, the theory of harm must ordinarily be dignitary or prophylactic. Part II of this Article addresses the problems with these theories of harm in data breach cases.

II. WHY DIGNITARY HARMS AND PROPHYLACTIC REMEDIES ARE NOT A PANACEA FOR DATA BREACHES

There should be some remedy for individuals who suffer demonstrable out-of-pocket losses because of a data breach, at least if the breach results from the negligence or contractual violation of the data processor or controller. But as the discussion in Part I shows, out-of-pocket losses linked to a specific data breach are relatively rare. This means that, any individual harm from the vast majority of breaches must be emotional, dignitary, or anticipatory of future out-of-pocket losses. The empirical, doctrinal, and evidentiary problems raised by these kinds of remedies, however, are for the most part prohibitory, at least in the context of commercial data breaches.

A. Empirical Questions

It is hard, if not impossible, to know whether or to what extent data breaches cause emotional harms. Some commentators and industry players have argued that emotional or dignitary harms from data breaches are acute and actionable.[144] According to a 2015 bulletin from the credit bureau

144. *See, e.g.*, Benjamin C. West, Note, *No Harm Still Foul: When an Injury-in-Fact Materializes in a Consumer Data Breach*, 69 HASTINGS L.J. 701, 717 (2018); MARISA SALCINES, EQUIFAX, A LASTING IMPACT: THE EMOTIONAL TOLL OF IDENTITY THEFT (2015), https://assets.equifax.com/legacy/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf.

Equifax, "identity theft victims may experience similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility."[145] The Equifax bulletin—designed to sell credit monitoring services—cites a study published by the Identity Theft Resource Center ("ITRC") in 2013.[146] The ITRC is a nonprofit organization supported by credit and Internet industry companies, a law firm, and a private foundation.[147] The 2021 version of the ITRC's *Consumer Aftermath Report* indicates that seventy-nine percent of survey respondents said they experienced "adverse feelings or emotions" as a result of identity theft.[148] The ITRC's work seems to confirm the intuition that identity theft is stressful for the victim.[149]

Other empirical studies, however, seem to reach more limited conclusions than the ITRC Report. A study concluded in the aftermath of the massive Equifax breach found that most people knew about the breach but did not take action because the costs were too high and the benefits of protective action too low.[150] On the "benefits" side, respondents did not seem excessively distressed about the possible consequences of the breach, and some respondents in fact felt they were not personally at risk.[151] Similarly, a recent study found that affected individuals were not even aware of most of the instances in which their PII was breached and expressed only "moderate"

145. *See* SALCINES, *supra* note 144.

146. *Id.* at 6.

147. *See* ITRC, 2020 ANNUAL REPORT: OVERCOMING UNIQUE CHALLENGES IN A PANDEMIC LANDSCAPE (2020), https://www.idtheftcenter.org/wp-content/uploads/2021/10/03.25.2020_2020-Annual-Report_FINAL-optimized.pdf.

148. ITRC, 2021 CONSUMER AFTERMATH REPORT: HOW IDENTITY CRIMES IMPACT VICTIMS, THEIR FAMILIES, FRIENDS, AND WORKPLACES 18, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf.

149. There are, however, many potential problems with the ITRC Report's scope and methodology. All individuals surveyed by ITRC for its 2021 Report "previously self-identified as being impacted by pandemic-related identity fraud" by contacting ITRC for assistance, an obvious selection bias. *Id.* at 2. A sidebar in the Report states that it is based on "427 individual victims of identity crimes out of the 5,571 victims [that were] offered the opportunity to participate," but the text on the same page states that the total number of individuals contacted was 752 and 63 of those contacted responded to the survey. *Id.* It appears that the first group of contacts dates from reported identity theft from 2017 to 2020, while the latter group dated from 2021, which the Report says covers "victims directly impacted by pandemic-related identity fraud." *Id.* at 4. The Report highlights that this response rate produced a margin of error of +/- 5% for the first group of responses and +/- 12% for the second group at a confidence level of 95%, but those figures are misleading. *Id.* at 2. Both figures assume that the number of people contacted by ITRC represent the relevant population size for calculating the sample margin of error. But the population surveyed entails an obvious selection bias in relation to any broader population of identity theft victims, so the margin of error tells us nothing about how these responses relate to the general population of such victims.

150. Yixin Zou et al., *"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach*, *in* PROCEEDINGS OF THE FOURTEENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 197 (USENIX Ass'n 2018), https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf.

151. *See id.* § 5.3, at 203–04.

concern about the breaches that involved their PII.[152] Likewise, the most recent Bureau of Justice Statistics *Victims of Identity Theft Report* concludes that only 8% of all identity theft victims reported the incident as "severely distressing."[153] Most (48%) experienced only "mild" distress, while 20% reported "none" and 23% reported "moderate" distress.[154] Not surprisingly, the largest category of severe distress was among people who experienced multiple types of fraud beyond existing account fraud.[155]

The prospect of payment card or new account fraud should not, then, cause the ordinary reasonable person substantial emotional distress. Undoubtedly, some consumers will become upset if they receive a bill for a line of credit they did not open, but significant emotional distress about such an event seems unreasonable.[156] A little bit of knowledge about how consumer credit works should assure the consumer that he or she will not incur any liability.[157] A reasonably informed consumer should know that the possibility of new account fraud, like the possibility of existing account fraud, is endemic to the consumer credit system in a world beset by the hard problem of computer crime and is offset by the credit benefit. In fact, this understanding already seems to have taken hold among the general public.[158]

It seems, then, that data breaches cause some degree of anxiety but whether this is on average significant or substantial is impossible to quantify. This empirical problem is related to the doctrinal issue discussed in the next Section. If an emotional or dignitary harm is actionable apart from physical or pecuniary losses, it must represent more than a general "background" anxiety arising from risks that most people face simply because the world is

152. Laurel Thomas, *Data Breaches: Most Victims Unaware When Shown Evidence of Multiple Compromised Accounts*, UNIV. MICH. NEWS (June 21, 2021), https://news.umich.edu/data-breaches-most-victims-unaware-when-shown-evidence-of-multiple-compromised-accounts/; Peter Mayer et al., *"Now I'm a Bit Angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them*, *in* PROCEEDINGS OF THE 30TH USENIX SECURITY SYMPOSIUM 393 (USENIX Ass'n 2021), https://www.usenix.org/system/files/sec21-mayer.pdf. This study utilized the "Have I Been Pwned?" database. *See supra* note 39.

153. HARRELL, *supra* note 120, at 11.

154. *Id.*

155. *Id.*

156. The BJS reports that victims of new account misuse and personal information misuse were more likely to report severe emotional distress than victims of existing account misuse. *Id.* "Misuse of personal information" was defined in this report as information "completed or attempted unauthorized use of personal information for fraudulent purposes, such as getting medical care, a job, or governmental benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation." *Id.* at 2.

157. It may be true that some consumers do not know that they are fully insured by the payment card system against fraudulent charges. This information is easy to discover, however, including through prominent portions of issuing bank websites. *See e.g.*, *supra* note 103. A reasonable consumer should know this basic fact.

158. *See supra* note 152.

never perfectly safe. Otherwise, the theory of liability is more akin to a kind of absolute enterprise liability—something tort law has eschewed in most other contexts.[159]

B. Is There a Trend Towards Dignitary Privacy Harms in Consumer Protection Statutes?

Notwithstanding these empirical problems, some scholars and authorities suggest that diverse strands of privacy law evince a trend towards recognizing emotional harms. The American Law Institute's text *Principles of the Law: Privacy* ("ALI PLP"), for which Professor Solove is the reporter, suggests that certain kinds of emotional harms should be actionable for various kinds of privacy violations.[160] This would include the possibility of future emotional harm.[161] The magnitude and likelihood of harm, according to the ALI text, should "fall along a sliding scale" based on both the likelihood and magnitude of potential harm.[162] A harm that is unlikely to occur but of potentially significant magnitude, the ALI text states, "may be a risk worthy of concern."[163] The extent to which there is a such a trend that would support a general "sliding scale," however, is questionable.

Comment c to the ALI PLP address emotional harm.[164] The comment references examples of hate crimes and unauthorized sharing of sexual photos and videos.[165] These are obviously traumatic circumstances, but they have little to do with most data breaches, and ordinarily do not seem to require a new legal rubric beyond well-established causes of action for intentional infliction of emotional distress.[166] An intentional or reckless disclosure of distressing information such as sexually explicit images falls into a different category than the exfiltration of consumer PII in a data breach that might have involved some lack of due care by a bank or merchant.

159. *See infra* Section III.A.

160. ALI PLP, *supra* note 8, § 14(d) & 14 cmt. c.

161. *Id.* § 14(e).

162. *Id.* § 14(d). This is in fact more like a matrix with two sliding scales.

163. *Id.*

164. *Id.* § 14 & cmt. c.

165. *Id.* (citing Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019)); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

166. Sometimes a data breach includes blackmail or doxing that might involve disclosure of information about a person's sex life, as in the Sony and Ashley Madison breaches. This is rare. The Sony breach was almost certainly a North Korean operation in retaliation for Sony's movie *The Interview*, which parodied North Korean dictator Kim Jong-un; the Ashley Madison breach involved a unique target—a website that facilitated adulterous affairs. *See supra* Part I. Cyberstalking, harassment, and sextortion usually involve individuals who know each other or isolated acts by specific individuals. It is not a kind of systemic cybercrime.

Comment c's other reference is to the Fair Debt Collection Practices Act ("FDCPA")[167] and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("TCFAP").[168] These statutes, comment c suggests, highlight "the emotional harm that can befall consumers" and authorize the Federal Trade Commission ("FTC") to engage in rulemaking "beyond traditional 'unfair' or 'deceptive' acts."[169] Such consumer fraud statutes might provide a more solid basis for emotional harms in data breach cases. A close examination of these statutes, however, shows that they have limited application and are mostly focused on objectively wrongful conduct rather than subject emotional harms.

The TCFAP, which was adopted in 1994, does refer to telemarketing activity "which the reasonable consumer would consider coercive or abusive of such consumer's right to privacy," but it does not mention subjective emotional distress.[170] The Telemarketing Sales Rule ("TSR") adopted by the FTC under the TCFAP "is fundamentally an anti-fraud rule."[171] However, one section of the TSR prohibits threats, intimidation, and the use of profane or obscene language in telemarketing.[172] The FDCPA similarly refers to "abusive, deceptive, and unfair debt collection practices," which, the statute says, "contribute to the number of personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy."[173] The statute covers how a debt collector may communicate with a consumer and, among other things, prohibits "any conduct the natural consequence of which is to harass, oppress, or abuse any person in connection with the collection of a debt."[174]

The ALI PLP and its comments assume that the harassment aspects of the TCFAP and FDCPA reflect a general recognition of emotional distress harms from invasions of privacy.[175] But these provisions are better understood as the regulatory side of law aimed at specific kinds of intentional conduct. A non-criminal regulatory statute need not satisfy traditional

167. Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692–1692p.

168. Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101–6108; ALI PLP, *supra* note 8, § 14, cmt. c.

169. ALI PLP, *supra* note 8, § 14, cmt. c.

170. *See* 15 U.S.C. § 6102(a)(3)(A).

171. Telemarketing Sales Rule, 80 Fed. Reg. 77,520, 77,520 (Dec. 14, 2015) (to be codified at 16 C.F.R. pt 310); Telemarketing Sales Rule, 60 Fed. Reg. 43,842–901 (Aug. 23, 1995).

172. 16 C.F.R. § 310.4(1).

173. 15 U.S.C. § 1692(a).

174. *Id.* § 1692d.

175. *See* ALI PLP, *supra* note 8, § 14.

criminal law principles relating to *mens rea*, but First Amendment concerns still apply, so provisions like the TSR's must be read narrowly.[176]

This concern arose in litigation over the TSR not long after it was amended in by the Patriot Act[177] in 2001 in response to fraudulent calls soliciting charitable donations for 9/11 victims.[178] In *National Federation of the Blind v. FTC*,[179] a group of charitable organizations challenged the constitutionality of this change.[180] The Fourth Circuit, applying Supreme Court precedent on regulations of charitable fundraising, examined whether the regulation (1) "'serves a sufficiently strong, subordinating interest that the [government] is entitled to protect' and (2) [was] 'narrowly drawn . . . to serve the interest without unnecessarily interfering with First Amendment freedoms.'"[181]

The FTC advanced two interests in support of the regulation: preventing fraud and protecting residential privacy.[182] The court noted longstanding precedent that preventing fraud is a sufficiently substantial interest.[183] The privacy interest advanced by the FTC specifically concerned *residential* privacy: "to allow family life to proceed undisturbed by phone calls in the evening and early morning hours."[184] The Fourth Circuit recited numerous precedents concerning the "sanctity of the home."[185] Although there is no general privacy right to be free of unwanted speech in public spaces, the court noted, "the home is different."[186] The court therefore agreed with the FTC that privacy within the home provided a substantial interest the government was entitled to protect.[187] The court further held that the regulations were sufficiently narrowly drawn because they applied only to particularly sensitive time periods when families might gather—breakfast and the end of the evening—which the court suggested are "the most personal hours of a family's day."[188]

176. *Cf.* Justin (Gus) Hurwitz, *Telemarketing, Technology, and the Regulation of Private Speech: First Amendment Lessons from the FCC's TCPA Rules*, 84 BROOK. L. REV. 1 (2018) (describing First Amendment issues arising from application of TCPA rules).

177. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

178. *See* Nat'l Fed'n of the Blind v. FTC, 420 F.3d 331, 335–36 (4th Cir. 2005).

179. 420 F.3d 331 (4th Cir. 2005).

180. *Id.* at 336.

181. *Id.* at 338 (first and third alterations in original) (quoting Sec'y of State of Md. v. Joseph Munson Co., 467 U.S. 947, 960–61, (1984)).

182. *Id.* at 339.

183. *Id.* (citing Riley v. Nat'l Fed'n of the Blind, 487 U.S. 781, 792 (1988)).

184. *Id.*

185. *Id.* at 340 (quoting Carey v. Brown, 447 U.S. 455, 471 (1980)).

186. *Id.* (quoting *Carey*, 447 U.S. at 471).

187. *Id.*

188. *Id.* at 341–43. According to the court:

A properly narrow reading of the TSR, as suggested by the Fourth Circuit in *National Federation of the Blind*, concerns privacy in the home, a domain considered special in the law since time immemorial.[189] This means the TCFAP and related statutes evince only a modest, quite traditional concern and not a broader trend towards emotional harms for privacy violations.

Other litigation over the meaning of the FDCPA likewise demonstrates that the statute focuses on an objective standard, not on subjective emotional harms. There has been plenty of litigation under the FDCPA's "harass, oppress, or abuse" provision, most of which concerns the meaning of those terms.[190] Courts have also struggled with the statute's "natural consequence" culpability standard.[191] Following the Second Circuit's holding in *Exposition Press, Inc. v. FTC*,[192] most circuits have adopted an objective "least sophisticated debtor" test for judging the impact of a potentially misleading or harassing statement under the FDCPA.[193] The kinds of practices considered harassing, oppressive, or abusive under the statute typically connect with other practices that could be fraudulent. In *Levins v. Healthcare Revenue Recovery Group*,[194] for example, the Third Circuit held that the plaintiffs stated a claim under the FDCPA's "true name" provision because the debt collector identified itself by a name that suggested it was an "account resolution service[]" rather than a debt collection agency.[195] However, the court upheld the dismissal of plaintiff's "harass, oppress, or abuse" claim because "[t]he voicemail messages [from the collection agency] provided enough information about the caller's identity for the least sophisticated debtor to know that the call was from a debt collector and was an attempt to collect a debt."[196]

Finally, although the basic standard under the FDCPA is objective and does not require a showing of intent, the "bona fide error" defense in the

> After 9:00 p.m., family members might, for example, be cleaning house for the night, bathing, paying bills, discussing homework, planning this or that, reading, watching TV, or simply getting ready to turn in. Before 8:00 a.m., they might be eating breakfast, dressing, shaving, or fixing lunch for spouses or kids. The First Amendment does not require us to interrupt these family moments, and the only burdens on speech imposed by the TSR time restrictions protect just the most personal hours of a family's day.

Id. at 341.

189. *See Riley*, 487 U.S. at 792.

190. 15 U.S.C.A. § 1692d (West) (notes of decisions 6, 8, and 9).

191. *Id.* § 1692d.

192. 295 F.2d 869 (2d Cir. 1961).

193. Levins v. Healthcare Revenue Recovery Grp. LLC, 902 F.3d 274, 280 (3d Cir. 2018); *see also* Exposition Press, Inc. v. FTC, 295 F.2d 869, 872 (2d Cir. 1961).

194. 902 F.3d 274 (3d Cir. 2018).

195. *Id.* at 280–81.

196. *Id.* at 282 (quoting 15 U.S.C. § 1692d).

statute states that a "debt collector may not be held liable in any action brought under this subchapter if the debt collector shows by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error."[197] The availability of this defense shows that the statue is aimed at specific practices and not at subjective emotional harms.

The TCFAP and FDCPA therefore provide little basis for the broad suggestion in comment c to the ALI PLP that U.S. privacy law widely recognizes emotional distress harms.[198] It is true that the TCFAP and FDCPA reflect some concerns about privacy within the home and about harassing and abusive practice connected with consumer fraud. In conjunction with criminal cyberstalking and cyber-harassment statutes, subject to limitations under the First Amendment, these kinds of provisions reflect a societal concern, expressed in particular legislative measures, about certain specific kinds of conduct. But these sources fall far short of an overarching norm in favor of tort claims for emotional distress arising from possibly negligent breaches of any sort of PII.

C. The Analogy to Anxiety and Emotional Distress Harms Without Physical Injury in Medical Negligence and Toxic Tort Cases

In addition to existing sources of privacy law, some privacy scholars have attempted to develop an emotional harms doctrine for privacy violations out of medical negligence and toxic tort jurisprudence. In an important set of articles, Professors Solove and Danielle Keats Citron have argued for recognition of "anxiety and risk" harms for privacy violations.[199] Solove and Citron note that courts require claimed data breach harms to be "visceral—easy to see, measure, and quantify"—and "vested—already materialized in the here and now."[200] They consider this a "cramped"[201] outlook and argue

197. 15 U.S.C. § 1692k(c).

198. ALI PLP, *supra* note 8, § 14 & cmt. c.

199. Solove & Citron, *Risk and Anxiety*, *supra* note 8, at 744. In an even more recent article, Solove and Citron expand their taxonomy of privacy harms. Citron & Solove, *Privacy Harms*, *supra* note 8, at 793. As with their *Risk and Anxiety* paper, most of the types of harms discussed are not specific to the data breach context. For example, under "physical harms," they discuss a woman who was murdered after a stalker obtained her address through a private investigator; under "economic harms" they discuss credit profiling by American Express; under "reputational harms" they discuss a program in which LinkedIn used user's contact lists to solicit new members; and so-on. *See id.* at 831–39. These may be important areas of harm to consider in different kinds of cases that are beyond the scope of this Article. In a section on "emotional distress," they cite to their *Risk and Anxiety* article, which is the main subject of the current Part of this Article. *Id.* at 841 n.277 (citing Solove & Citron, *Risk and Anxiety*, *supra* note 8, at 746).

200. Solove & Citron, *Risk and Anxiety*, *supra* note 8, at 754.

201. *Id.*

that courts should recognize "risk" and "anxiety" as "the key dimensions of data-breach harms."[202]

Under the "risk" category, Solove and Citron observe that it can take significant time between the discovery of a data breach and when the stolen PII is used in a way that economically harms the individual victim.[203] Because of the risk that a credit report might become compromised, they suggest, an individual may put off important decisions such as applying for a job or buying a home.[204] They analogize this kind of risk to the sale of a safe when the combination already has been publicly disclosed, or to the contraction of a virus that may later cause the infected person to develop a painful disease but that may also cause no symptoms of illness.[205] Under the "anxiety" category, Solove and Citron suggest the knowledge that "personal information, often sensitive, can be observed and used to one's detriment" should be a form of cognizable emotional harm even absent any accompanying physical, property, or economic harm.[206]

Solove and Citron argue that the "risk" and "anxiety" harms arising from a data breach are analogous to other kinds of privacy or medical malpractice torts in which courts have allowed claims for damages without present physical, property, or economic harms.[207] There are several significant problems with this argument.

First, the weight of authority does not support a trend towards increased recognition of "anxiety" or emotional distress harms based on foreseeability alone. For example, as Solove and Citron note, the California Supreme Court recognized a claim for negligent infliction of emotional distress without accompanying physical harm in *Molien v. Kaiser Foundation Hospitals*.[208] *Molien*'s holding, however, subsequently was cabined in *Burgess v. Superior Court*.[209] In *Burgess*, the California Supreme Court noted that *Molien* had been subject to significant criticism "centered upon the perception that *Molien* introduced a new method for determining the existence of a duty, limited only by the concept of foreseeability."[210] This perception, the *Burgess* court said, was mistaken.[211] According to *Burgess*, damages for emotional harm are recoverable absent physical harm or impact only if they are caused

202. *Id.* at 756.
203. *Id.*
204. *Id.* at 759.
205. *Id.* at 759–60.
206. *Id.* at 764.
207. *Id.* at 768–69.
208. 616 P.2d 813 (Cal. 1980); *see* Solove & Citron, *Risk and Anxiety*, *supra* note 8, at 768, 769 n.177.
209. 831 P.2d 1197 (Cal. 1992).
210. *Id.* at 1201
211. *Id.*

by "a duty arising from a preexisting relationship" that has been breached.[212] Further, according to *Burgess*, absent accompanying physical harm, a plaintiff can recover damages for emotional distress only if the distress is "*serious*."[213] *Burgess*' limitations on *Molien* are consistent with the trend in other jurisdictions.[214]

Second, consistent with the suggestion in cases such as *Burgess* that emotional distress damages are only recoverable absent physical harm if they are "serious," the categories of cases in which courts have allowed such claims tend to involve areas in which there are widespread and longstanding norms and expectations about propriety and harm. For example, some courts have allowed emotional distress damages to close relatives for the publication of death images or videos even if the plaintiff does not appear in the image or video.[215] The "death image" cases reflect social norms arising from time immemorial, embedded deep in the common law, concerning burial rites and a family's dignity interests relating to deceased relations.[216] "Risk" or "anxiety" harms arising from data breaches are a product of the Internet and e-commerce, phenomena that did not exist in time immemorial. If anything, the Internet and e-commerce have rapidly established social norms that accept widespread public sharing of personal information, particularly among digital natives.[217]

Third, the "risk" cases involve at least two different kind of negligence damages, both presenting their own problems in the data breach context. A plaintiff can sometimes recover present damages for a future risk of harm as an element of present harm. Part of the rationale for this sort of recovery is judicial efficiency: A different rule would require the plaintiff to file new lawsuits every time some further aspect of harm is realized.[218] A key question in such cases is whether a plaintiff can prove that future harm is reasonably

212. *Id.*

213. *Id.* at 1205 (quoting *Molien*, 616 P.2d at 819–20).

214. *See* 4A STUART M. SPEISER, CHARLES F. KRAUSE & ALFRED W. GANS, THE AMERICAN LAW OF TORTS § 16:12 (Monique C.M. Leahy ed., 2016) (noting limitations, and in some states bans, on recovery of emotional distress damages absent physical harms).

215. *See, e.g.*, Catsouras v. Dep't of Cal. Highway Patrol, 104 Cal. Rptr. 3d 352, 373–74 (Ct. App. 2010) (citing Christensen v. Superior Court, 820 P.2d 181, 197–98 (Cal. 1991)).

216. *See id.* at 363–64; Nat'l Archives & Recs. Admin. v. Favish, 541 U.S. 157, 167–69 (2004) (upholding family's privacy interest in death image sought under FOIA request and stating that "[b]urial rites or their counterparts have been respected in almost all civilizations from time immemorial").

217. *See, e.g.*, Nicholas Proferes, *The Development of Privacy Norms*, *in* MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY 79 (Bart P. Knijnenburg et al. eds., 2022); Xinru Page et al., *Social Media and Privacy*, *in* MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY, *supra*, at 113.

218. *See* Petriello v. Kalman, 576 A.2d 474, 483 (Conn. 1990) (noting that "[i]n seeking to enforce their right to individualized compensation, plaintiffs in negligence cases are confronted by the requirements that they must claim all applicable damages in a single cause of action").

probable rather than speculative or merely possible.[219] In the past, many states adopted an "all or nothing" rule that required proof that the future harm was more likely than not—a chance above fifty percent—to occur.[220] Some states have shifted to a rule that applies the percentage chance of occurrence, even if below fifty percent, against the putative damage amount.[221] In some states, a plaintiff can also claim present emotional distress damages for a *reasonable fear* of future harm.[222] The question of what comprises a *reasonable* fear presents issues of proof similar to the assessment of future physical damages.[223]

These questions of proof about future harm often can be addressed effectively in tort cases involving physical injury. Medical experts can offer scientifically supported estimates about the probability of future complications from present injuries. Such estimates might be inexact, and experts for the different parties might disagree, but there is usually some basis for an informed jury decision.

This is not so easy in data breach cases. As discussed in Part I, it seems that most of the time individuals do *not* suffer any ascertainable losses when their PII is part of a data breach. Understanding the computer crime ecosystem, we can see why this makes perfect sense. There is no way to know whether or when any individual's PII taken in any specific data breach will be used to engage in any of the criminal activities, such as credit card fraud, that comprise the computer crime ecosystem. At the same time, nearly everyone who lives and works and does commerce in cyberspace will, at some point, have to deal with an unauthorized payment card charge or strange item on a credit report. To return to the toxic tort analogy, it is like observing that there are levels of potentially harmful plastics in most of our groundwater where the specific sources of the plastic waste are vast and impossible to pinpoint in any one instance.[224] Some degree of anxiety about the problem is appropriate, but there is no way to tie that anxiety to one catastrophic plastic spill. It is systemic, not individualized, harm.

Further, although payment card information is PII, it does not in itself have any emotional valence. When a card number and associated name, address, and CCV number are entered into a merchant's purchase page, that information is automatically transmitted through the merchant's payment system to the merchant's acquiring bank, and then by the merchant's

219. *See, e.g.*, *id.* at 481–85.

220. *Id.* at 482.

221. *Id.* at 483.

222. *Id.* at 481.

223. *See id.* at 480–81.

224. *See* Mary Kosuth et al., *Synthetic Polymer Contamination in Global Drinking Water*, ORB MEDIA (May 16, 2017), https://orbmedia.org/invisibles-final-report.

acquiring bank to cardholder's issuing bank.[225] The issuing bank confirms the purported validity of the transaction and authorizes the payment in accordance with the cardholder's credit line, which is processed to the merchant through the acquiring bank. This happens almost instantaneously, literally at the speed of light (or at least, where there are no fiberoptic cables, at the speed of electricity).[226] No human being views any of this information as the transaction happens. Much of this processing happens on dedicated networks purpose-built by the card brands, not on the public Internet, although even the information that travels over the public Internet is encrypted.[227]

The payment card system is almost incomprehensively massive. There are billions of such transactions happening every day.[228] In these circumstances, a person's name, address, and CCV number are nothing special. It is just information reduced to code that computers use to enable the credit benefit. If there is a dignitary harm to individual consumers, then, most of it is built into the credit system itself. The credit system cannot function efficiently unless banks amass large amounts of sensitive personal information about their customers. The modern economy could not function without the credit benefit. Fraud cannot entirely be prevented, so the risk of some degree of fraud is already built into the system through the reimbursement requirement. For most of us, at least this much indignity is outweighed by the value of the credit benefit.

True identity theft, in contrast to payment card fraud, could understandably produce more tangible emotional distress, because it can be more difficult to untangle. For a reasonably knowledgeable person in the digital age, however, this distress should not ordinarily be severe, absent exceptional circumstances.[229] A credit freeze and a few messages and phone calls will fix most low-level identity theft if it is not already screened by the credit bureaus and other financial services firms based on their fraud detection algorithms.[230] This is annoying and unpleasant, but it to be expected in cyberspace. If an identity theft situation becomes unusually persistent and difficult to remedy, serious emotional distress is more reasonable, although

225. *See* Rebecca Lake, *What is a Credit Card Network?*, BALANCE (May 4, 2022), https://www.thebalance.com/what-is-a-credit-card-network-4775633.

226. *See Science of Glass: How it Works – Optical Fiber*, GLASS AGE, https://www.corning.com/worldwide/en/innovation/the-glass-age/science-of-glass/how-it-works-optical-fiber.html (last visited Apr. 10, 2023).

227. *See generally VisaNet. A Network you Can Trust.*, VISA (last visited Mar. 6, 2023), https://usa.visa.com/about-visa/visanet.html.

228. *Id.*

229. *See supra* Sections I.C.1–3.

230. *See supra* Section I.C.4.

in such circumstances the emotional distress will accompany quantifiable out of pocket losses and therefore will fall neatly into traditional tort doctrines.

Synthetic identity theft, in contrast, should not produce any emotional distress at all because an individual whose PII was used to construct a synthetic identity typically will not know the difference.[231] It feels creepy that cybercriminals could use parts of my PII to construct a fake person, but the creepy feeling seems to have no rational basis in concerns about my individual welfare, apart from the knowledge that this activity drains wealth from the broader economy.

The remaining major categories of commercial cybercrime—market manipulation, trade secret theft, and state surveillance—are even less likely to produce emotional harms without pecuniary losses that could be remedied by private law.[232] Market manipulation may cause significant emotional distress to a person whose brokerage account was depleted if the brokerage firm does not readily agree to reimburse the client, but this would involve pecuniary as well as dignitary harms.[233] An individual claim for dignitary harm apart from pecuniary harm seems untenable if the firm readily remedies any losses. Trade secret theft does not usually target PII so individual remedies ordinarily are not at issue in such cases. State surveillance is undoubtedly frightening, but it is far beyond the reach of private law remedies.

In sum, then, a general category of dignitary or emotional harm is a poor doctrinal and practical fit for most kinds of data breaches.[234]

D. Prophylactic Remedies: Credit Monitoring and the Analogy to Medical Monitoring

Although damages for fear of future harm are still rare in data breach cases, some courts have allowed negligence and related claims to proceed on the merits for breaches facilitated by malware if the plaintiff has incurred demonstrable time and expense costs. Such costs might include payments for credit monitoring insurance, even absent a showing of any present misuse of the plaintiff's personal information.[235] This is subtly different than a remedy for fear of future harm. The remedy for fear of future harm provides damages for emotional distress. The remedy for monitoring expenses covers out-of-pocket costs reasonably expended to mitigate a reasonable probability of

231. *See supra* Section I.C.3.

232. *See supra* Section I.C.3.

233. *See supra* Section I.C.3.

234. *See supra* Section I.C.3.

235. *See, e.g.*, Castillo v. Seagate Tech., LLC, No. 16-cv-01958-RS, 2016 WL 9280242, at *2 (N.D. Cal. Sept. 14, 2016).

future harm.[236] Of course, if a person spends money to prevent a potential future harm, there is presumably some degree of fear and anxiety motivating that expenditure. The damage award, however, is tied to specific expenses reasonably related to mitigating physical or property harm for which the plaintiff is at greater risk because of the defendant's negligence.

As this summary suggests, this kind of remedy developed in the context of medical monitoring expenses in toxic tort cases. It has been endorsed by some commentators in the data breach context.[237] In nearly every court-approved settlement of a data breach consumer class action, credit monitoring insurance for class members is a core element of the settlement package.[238]

Notwithstanding its popularity as a part of data breach class action settlements, there is scant analysis of this remedy in the data breach case law. An exception is *Corona v. Sony Pictures Entertainment, Inc.*,[239] in which Judge R. Gary Klausner of the United States District Court for the Central District of California discussed, in deciding a rule 12(b)(6) motion, plaintiffs' claims for costs actually incurred for credit monitoring and other prophylactic measures after the infamous Sony breach.[240] Judge Klausner first rejected plaintiffs' claims for "future harm or an increased risk in harm that has not yet occurred" as well as plaintiffs' "general allegations of lost time."[241] According to Judge Klausner, those claims were "too speculative to constitute cognizable injury."[242]

As to plaintiffs' actual out-of-pocket costs for credit monitoring insurance and documented lost time, however, Judge Klausner found that California's toxic tort medical monitoring law was analogous.[243] Based on the medical monitoring cases, Judge Klausner determined that the following five factors should apply:

(1) the significance and extent of the compromise to Plaintiffs' PII;
(2) the sensitivity of the compromised information; (3) the relative

236. *See, e.g.*, Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 821–25 (Cal. 1993).

237. *See* Solove & Citron, *Risk and Anxiety*, *supra* note 8.

238. *See* Opderbeck, *supra* note 4.

239. No. 14-CV-09600, 2015 WL 3916744 (C.D. Cal. June 15, 2015).

240. *Id.* at *4. A case presently working through the United States District Court for the Northern District of California, *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633 (N.D. Cal. 2020), provides another illustration. *Id.* at 650. Plaintiff Huynh testified at her deposition that she spent about one hour per day checking her information after learning of the breach and that she purchased credit monitoring insurance. *Id.* at 643–44. She did not, however, experience any fraudulent charges or other misuse of her PII. *Id.* The trial judge cited the *Corona* court's application of California's toxic tort medical monitoring cases to data breaches and held that Hunyh's claims survived summary judgment. *Id.* at 650.

241. *Corona*, 2015 WL 3916744, at *4.

242. *Id.*

243. *Id.*

> increase in the risk of identity theft when compared to (a) Plaintiffs' chances of identity theft had the data breach not occurred, and (b) the chances of the public at large being subject to identity theft; (4) the seriousness of the consequences resulting from identity theft; and (5) the objective value of early detection.[244]

The court found that the sensitivity of the compromised information, which included Social Security numbers, health insurance, and banking information, specific evidence that the exfiltrated data had been posted to torrent sites, the public release of some of the information (a form of doxing), and a threat from the hackers to release more information, satisfied these factors.[245]

The factors applied by Judge Klausner were derived from *Potter v. Firestone Tire & Rubber Co.*,[246] a case which established a cause of action for medical monitoring in California.[247]

The California Supreme Court in *Potter* articulated four important policy concerns in favor of medical monitoring claims.[248] These included: (1) the public health interest where toxic chemicals create an increased risk of disease, "particularly in light of the value of early diagnosis and treatment for many cancer patients"; (2) deterring "irresponsible discharge of toxic chemicals"; (3) the prevention or mitigation of serious illness that would impose further costs on all the parties; and (4) "societal notions of fairness and elemental justice."[249] The *Potter* factors were designed to create "substantial evidentiary burdens for toxic exposure plaintiffs" so that plaintiffs cannot recover for the kinds of medical checkups "an individual should pursue as a matter of general good sense and foresight."[250] The factors are:

> (1) the significance and extent of the plaintiff's exposure to the chemicals; (2) the relative toxicity of the chemicals; (3) the seriousness of the diseases for which plaintiff is at an increased risk; (4) the relative increase in the plaintiff's chances of developing a disease as a result of the exposure, when compared to (a) plaintiff's chances of developing the disease had he or she not been exposed, and (b) the chances of members of the public at large developing the disease; and (5) the clinical value of early detection and diagnosis.[251]

244. *Id.* (citing Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824 (Cal. 1993)).
245. *Id.* at *4–*5.
246. 863 P.2d 795 (Cal. 1993).
247. *Id.* at 823–24.
248. *Id.* at 824.
249. *Id.* (quoting *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 852 (3d Cir. 1990)).
250. *Id.* at 825.
251. *Id.* at 823.

Judge Klausner's adaptation of the *Potter* factors represents a principled effort to extend existing standards regarding monitoring and potential future harm to the data breach context. The comparison between medical monitoring after exposure to toxic chemicals and cyber monitoring after a data breach, however, breaks down almost immediately. The *Potter* court held that plaintiff must demonstrate "the necessity, as a direct consequence of the exposure in issue, for specific monitoring beyond that which an individual should pursue as a matter of general good sense and foresight."[252] The *Potter* factors connecting the extent of exposure, increased risk of illness, seriousness of potential illness, and clinical value of monitoring, relate to established medical knowledge and standards of care.[253] Further, medical monitoring cases usually recognize that nearly everyone in modern society is regularly exposed to some level of carcinogens and other potentially harmful substances.[254] A plaintiff therefore must demonstrate exposure and risk significantly beyond ordinary background levels resulting from a defendant's negligence.[255]

There are no analogous standards relating to the exposure of an individual's PII in a data breach. Regular exposure of PII to third parties is and always has been necessary for life and commerce. As the data summarized in Part I suggests, the exposure of PII in commercial data breaches is also now a background fact of life for most people. It is therefore difficult to see how any individual data breach exposes an individual to a significantly marginally greater potential for future harm than the background risk of harm from cybercrime generally. The purchase of identity theft insurance might be a reasonable expenditure in general, but it seems difficult to connect this cost with a particular breach notice. It is more analogous to getting an annual checkup and making sure one's standard vaccinations are up to date than to special tests for cancers that might result to unusual exposure to toxic waste that does not touch most of the population.

In addition, even with this substantial background risk, much depends on what the insurance covers. Some of the services offered by typical identity protection insurance plans are already available for free. This includes the ability to obtain free credit reports, freeze a credit file, and obtain fraud relief from payment card providers.[256] The main value-adds of commercial identity

252. *Id.* at 825 (quoting Miranda v. Shell Oil Co., 15 Cal. Rptr. 2d 569, 660 (Ct. App. 1993)).

253. *Id.* at 816.

254. *Id*. at 825; *see also In re Paoli*, 113 F.3d at 459 (upholding a jury instruction stating that exposure "in amounts significantly beyond what would enter a person's body in everyday life elsewhere in the [relevant] area and in amounts sufficient to cause the plaintiff to have a risk of future disease significantly greater than what he or she would have had without exposure").

255. *See In re Paoli*, 113 F.3d at 459.

256. *See* Sean Pyles & Bev O'Shea, *Do You Need Identity Theft Protection Services?*, NERDWALLET (Jan. 25, 2022), https://www.nerdwallet.com/article/finance/comparing-identity-

theft insurance providers include: (1) proactive monitoring and notifications of new credit reporting information (an extra value, if at all, because the information is automatically delivered to the consumer), (2) monitoring of information on the dark web, and (3) cash insurance benefits of up to $1 million for certain expenses including lawyer costs, expert costs, and fund reimbursements.[257]

Of course, like any insurance policy, the value of the cash coverage depends on the policy contract's details. Norton-Lifelock's policy contract, for example, reimburses for "stolen funds" but defines that term to exclude "any amount for which You did not seek reimbursement from the Financial Institution which holds the Account from which funds were stolen, and any amount for which You are (or would have been but for coverage under this Policy) eligible to receive reimbursement from any other source."[258] Since issuing banks are required to reimburse any fraudulent payment card charges, and personal bank accounts at major banks are insured for up to $250,000 by the Federal Deposit Insurance Corporation ("FDIC"), it is difficult to imagine any circumstance in which a typical consumer would qualify for reimbursement under this policy.[259] Data protection policies also usually contain "War or Terrorism" exclusions, which could exclude recovery for data breaches connected with organized crime groups and state actors.[260] These policies further exclude claims arising from the policyholder's negligence. Norton-Lifelock's policy defines policyholder negligence as "the failure to exercise reasonable care with respect to the disclosure of or providing access to personally identifiable information, an Account, or Theft of a handbag, purse or wallet."[261] It is unclear what duties of monitoring and remediation this clause places on policyholders. Commercial identity theft protection, then, might provide some marginal benefits to consumers, but those benefits are likely to be quite small and unrelated to any individual data breach.

In summary, like dignitary and emotional distress remedies, prophylactic remedies are a weak doctrinal fit for most commercial data

theft-protection-services. For a free U.S. government website that helps victims of data breaches implement a recover plan, see IDENTITYTHEFT.GOV, https://www.identitytheft.gov (last visited Apr. 24, 2023).

257. Pyles & O'Shea, *supra* note 256.

258. *See generally Evidence of Coverage: All Members Except NY and WA State Residents*, NORTONLIFELOCK, https://www.nortonlifelock.com/us/en/legal/unitedspeciality48-Sept2020/ (last visited Mar. 7, 2023).

259. *Deposit Insurance*, FED. DEPOSIT INS. CORP. (Mar. 15, 2023), https://www.fdic.gov/resources/deposit-insurance/; *see supra* Section I.B.1.

260. *Evidence of Coverage: All Members Except NY and WA State Residents*, *supra* note 258 (at header "War on Terrorism").

261. *Id.* (at header "Your Negligence").

breach incidents and do little to benefit individuals whose PII were part of a breach.

III. SYSTEMIC HARMS, SYSTEMIC MEASURES

Parts I and II of this Article argue that dignitary, emotional distress, and prophylactic remedies are a poor fit for most commercial data breach cases, at least with a clear showing of individual pecuniary loss tied to a specific breach. At this point in the history of cyberspace, the risks of data breaches are systemic. Because of the credit benefit and other benefits of electronic commerce, reasonable consumers will continue to disclose PII to banks, merchants, social media companies, and other enterprises. Because of the sophistication, social structures, and ubiquity of commercial cybercrime, reasonable consumers should reasonably assume that some of their PII will end up on the dark web. And because the market, particularly in the financial services industry, contractually adjusts for most of the risks of commercial cybercrime, a reasonable consumer should not become excessively distressed about any given data breach notice. A reasonable consumer might buy identity theft insurance to mitigate some commercial data breach risks but might also conclude that these insurance policies provide small marginal benefits over what the market provides already.[262]

Theories about individual dignitary and emotional harms and prophylactic remedies for data breaches therefore fall apart factually and doctrinally absent tangible pecuniary losses tied to a specific incident. In essence, such theories attempt to impose a kind of enterprise liability on every bank and merchant ever subjected to a data breach in which consumer PII was exfiltrated. Enterprise liability was introduced into the mass tort context by Judge Jack B. Weinstein in *Hall v. E.I. Du Pont De Nemours & Co.*[263] The court in *Hall* held that an industry was liable as a whole for damages that could not be traced back to a single defendant.[264] Although some courts in toxic tort cases have adopted modified versions of enterprise liability, such as market share liability, the concept has been rejected by most courts in most kinds of cases.[265] Most courts recognize that enterprise liability attempts to impose broad regulatory policies that should be enacted by legislatures and overseen by executive branch agencies rather than managed by courts through tort law and class action settlements. [266] But absent shaky

262. *See supra* notes 256–261 and accompanying text.

263. 345 F. Supp. 353 (E.D.N.Y. 1972).

264. *Id.* at 378.

265. *See* 1 MICHAEL DORE, LAW OF TOXIC TORTS § 6:5, Westlaw (database updated Mar. 2023).

266. *See, e.g.*, Sindell v. Abbott Lab'ys, 607 P.2d 924 (Cal. 1980) (market share theory); Martin v. Abbott Lab'ys, 689 P.2d 368 (Wash. 1984) (rejected by *Mulcahy v. Eli Lilly & Co.*, 386 N.W.2d

theories of emotional harm that lead to a kind of enterprise liability in tort litigation, what can be done to mitigate the systemic risk of data breaches? As the next Section shows, scholarly opinion varies, but there seems to be a growing consensus around a mix of regulatory rules and standards.

A. Scylla and Charybdis: Abandon All (Most) Hope or Private Law Strict Liability?

Some scholars suggest not only that data breaches are a poor fit for private litigation but also that cybersecurity is a poor fit for governmental regulation or legal standards aimed at prevention. In a series of early (in Internet years) articles, Derek Bambauer argues that efforts to prevent cyberattacks are mostly fruitless, and that energy should instead be put into resilience through disaggregation, redundancy, and diversifying software.[267] More recently, in a paper that seems to recognize that some cyber-defense is necessary, Bambauer argues that the FTC should exercise a prominent role in cybersecurity regulation through *per se* standards focused on obvious mistakes such as insecure passwords like "solarwinds123."[268] In *Cybersecurity for Idiots*, curiously, in light of his previous skepticism about defensive cybersecurity, Bambauer cites William McGeveran's article, *The Duty of Data Security*, for examples of "worst practices" that could provide evidence of a violation of this *per se* duty.[269]

McGeveran contends that arguments against the feasibility of developing cybersecurity standards of care are "balderdash."[270] McGeveran identifies a number of industry and governmental frameworks, such as the NIST Framework and Payment Card Industry Data Security Standard, along

67 (Iowa 1986), defining market share-alternate liability theory); Collins v. Eli Lilly Co., 342 N.W.2d 37 (Wis. 1984) (rejected by *Gullotta v. Eli Lilly & Co.*, No. CIV.H-82-400, 1985 WL 502793 (D. Conn. May 9, 1985), and *Mulcahy*, 386 N.W.2d 67, market share theory, suit of one defendant permitted); Conley v. Boyle Drug Co., 570 So. 2d 275 (Fla. 1990) (market share-alternate liability theory); Sheffield v. Eli Lilly & Co., 192 Cal. Rptr. 870, 883 (Ct. App. 1983) (finding that the plaintiffs failed to show an inadequate industry-wide standard of safety regarding the Salk polio vaccine); Starling v. Seaboard Coast Line R.R. Co., 533 F. Supp. 183 (S.D. Ga. 1982) (applying Georgia law); Griffin v. Tenneco Resins, Inc., 648 F. Supp. 964 (W.D.N.C. 1986) (applying North Carolina law); Zafft v. Eli Lilly & Co., 676 S.W.2d 241, 245–47 (Mo. 1984). According to the *Zafft* court, enterprise liability would "discourage desired pharmaceutical research and development while adding little incentive to production of safe products." *Zafft*, 676 S.W.2d at 247. In *Zafft*, which involved DES, the court also rejected enterprise liability because of the large number of manufacturers involved, the lack of delegation of responsibility for safety to a trade association, and the pervasive role played by the Food and Drug Administration. *Id.* at 245.

267. Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 587, 645–60 (2011); Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1012, 1052–62 (2014).

268. Bambauer, *supra* note 43, at 172.

269. *Id*. at 193–94 (citing William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019)).

270. McGeveran, *supra* note 269, at 1137.

with a number of legal frameworks, such as state data breach notification laws, as the basis for a flexible standard of reasonable care for cybersecurity.[271] McGeveran's frameworks include both necessary practices, such as regular security audits, and worst practices to be avoided, such as failure to install patches.[272] He offers the HIPAA Security Rule as a good example of a risk-benefit analysis, akin to the Learned Hand balancing test, that incorporates recognized security frameworks.[273]

Gus Hurwitz argues that McGeveran's effort to distill a meaningful duty of care for cybersecurity fails to identify any objective standards.[274] Hurwitz argues that cybersecurity standards are inherently subjective because they always refer to what is appropriate for a specific company's size and business.[275] Hurwitz suggests that if the purpose of a cybersecurity standard of care is to improve security practices, that purpose will fail because of the rapidly evolving, opportunistic, and adversarial nature of cybercrime.[276] According to Hurwitz, "[i]mposing an objective duty of data security . . . may vindicate some carnal sense to vindictive or retributive justice; in occasional cases it may lead to compensatory damages to make a random sample of affected consumers whole; but it will not meaningfully improve the state of data security."[277] He proposes the following standard, which he considers a kind of "subjective" reasonableness: "Did the firm invest in security in proportion to its size, complexity, resources, risk tolerance, and generally its understanding of its exposure to risk of attack?"[278]

It is helpful to compare Bambauer, Hurzwitz, and McGeveran. There is something fundamentally correct about Bambauer's observation that because defensive cybersecurity is always just out of reach, legal standards or rules focused on defensive cybersecurity are problematic. Bambauer's focus on disaggregation and redundance makes sense in response to some kinds of cybersecurity risks—in particular, ransomware. But this focus stands in severe tension with other basic privacy and cybersecurity principles. The Fair Information Practice Principles ("FIPPs") and the GDPR call for data *minimization*, which contradicts a call for redundancy, at least concerning

271. *Id.* at 1141.

272. *Id.* at 1175–95.

273. *Id.* at 1204–07.

274. Justin (Gus) Hurwitz, Response, *Response to McGeveran's* The Duty of Data Security*: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need*, 103 MINN. L. REV. HEADNOTES 139 (2019).

275. *Id.* at 145–47 (quoting the FTC's order in *LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2011) requiring LabMD to adopt safeguards "appropriate to [its] size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers").

276. *Id.* at 152.

277. *Id.*

278. *Id.* at 153.

PII.[279] The "I" and "A" of the CIA triad—confidentiality, integrity, and availability—can also be compromised if the means of achieving disaggregation and redundancy pose risks of hard to locate, missing, or conflicting copies of data records.[280] There is always a balancing act between defensive measures that seek to protect against successful attacks, measures designed to defend against and mitigate attacks in progress, and measures designed to recover from the inevitability of successful attacks—reflected in the NIST Framework of Identify, Protect, Defend, Respond, Recover.[281]

Nevertheless, Bambauer's skepticism of defensive cybersecurity coheres with Hurwitz's correct contention that cybersecurity standards must always account for the specific—in Hurwitz's (odd, if not mistaken) word, "subjective"—circumstances.[282] Your local neighborhood pizza shop with a website cannot be expected to invest the same amount in defensive cybersecurity as McDonald's with its multi-billion-dollar global business. Your main street two-person country law firm cannot be expected to invest the same amount in cybersecurity as Kirkland & Ellis.[283] But, the pizza shop and the two-person country law firm certainly should invest *something* in defensive cybersecurity, and the law firm probably should invest more than the pizza shop because of the more sensitive nature of the PII it holds.

Contrary to Hurwitz's characterization, this kind of context-sensitive risk management is not "subjective."[284] It is objectively reasonable that the "B" in the famous Learned Hand $B >< PL$ formula must reflect the burden to the specific party.[285] A risk management framework that would require an entity to bankrupt itself is not objectively reasonable, unless the only

279. *See Fair Information Practice Principles*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/article/fair-information-practices/ (last visited Mar. 7, 2023); Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) art. 5(1)(c) ("Personal data should be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')").

280. *See* SANS Institute, *CYA by Using CIA—Correctly For a Change | SANS@MIC Talk*, YOUTUBE, at 7:00–12:00 (June 9, 2020), https://www.youtube.com/watch?v=BmSZFHQg2zA (noting that "everyone in cybersecurity has heard of the CIA triad").

281. *See* Amy Mahn, *Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework*, NIST: TAKING MEASURE (Oct. 23, 2018), https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework.

282. *See* Hurwitz, *supra* note 274, at 153.

283. Kirkland & Ellis is as of this writing the world's largest law firm by revenue with over $4.8 billion in annual revenue. Shobhit Seth, *Top 10 Largest Law Firms in the World*, INVESTOPEDIA (Oct. 29, 2022), https://www.investopedia.com/articles/personal-finance/010715/worlds-top-10-law-firms.asp.

284. *See* Hurwitz, *supra* note 274, at 153.

285. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947). "B" is the burden of taking precautions, "P" is the probability of loss, and "L" is the amount of loss. *See id.*

reasonable outcome is to put the entity out of business because the social benefits of that entity's business are outweighed by risks that can feasibly be mitigated. In other words, the background of the Hand formula is not only the absolute quantitative comparison of B and PL, but also the overall social utility of the allegedly negligent party's activity in relation to the risk of harm.[286]

To use the *United States v. Carroll Towing Co.*[287] example, we know the cost of keeping a radio on a docked ship, but we can never fully calculate the probability and extent of every possible type of harm that could ensue if a docked ship breaks loose from its mooring without a radio.[288] We may have a knowable L from a specific collision in the harbor, and in retrospect the P will always be close to a value of one, but from the perspective of a prospective duty, without a large amount of repeatable underwriting data, the formula is basically a guess. We could prospectively set P and L so high that docking at harbor would require expensive twenty-four-hour crews and costly automated warning systems, but that would destroy the overall social utility of a robust and diverse shipping fleet. It is reasonable, all things considered, to impose smaller burdens—an inexpensive radio—on smaller ships.

McGeveran, then, is correct that the frameworks he identifies, which account for the specific circumstances of a target company, utilize a concept of objective reasonableness. But what Hurwitz is really pointing out is that the huge diversity of actors in cyberspace means that it is almost impossible to glean generally applicable rules or standards from these frameworks. A harbor, even in the wartime context of *Carroll Towing* or in the much bigger context of today's massive container ship fleets, is a manageably closed set. There are only so many kinds of ships, so many kinds of uses for ships, and so many kinds of dockages. Tort duties of care can help push a discrete set of safety standards that are reasonable in relation to classes of vessels within the context of a known universe of maritime commerce. But businesses as diverse as your corner pizza shop and the global law firm Kirkland & Ellis, and everything below, above, and between, are anchored in cyberspace. It

286. *See* Richard A. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29, 32–33, 41, 46, 76 (1972) (discussing the Hand formula as a way of estimating systemic social welfare). For a discussion of varying views about this economic theory of negligence and alternative theories, see, for example, Christopher Brett Jaeger, *The Empirical Reasonable Person*, 72 ALA. L. REV. 887, 902–10 (2021); Stephen G. Gilles, *The Invisible Hand Formula*, 80 VA. L. REV. 1015, 1016–37, 1039–44, 1052–54 (1994).

287. 159 F.2d 169 (2d Cir. 1947).

288. *See id.* at 172–74.

seems impossible to generalize without excluding some classes of otherwise legitimate business from cyberspace altogether.[289]

Hurwitz has argued that the difficulties of using a negligence duty of care for cybersecurity counsels in favor of strict liability.[290] He suggests that strict liability is a "relatively simple mechanism" that can remedy the risk-benefit, causation, and bargaining power problems raised by tort- and contract-based approaches.[291] He further argues that existing public law solutions, while potentially helpful, are limited by a focus on consumer protection rather than on systemic risk.[292]

Hurwitz recognizes that a strict liability regime would not address the problem of proving harm.[293] He suggests that this could be remedied through "statutorily directed" damages, by which he means lower burdens of proof and a published schedule of damages, much like a worker's compensation regime.[294] This strict liability regime, in Hurwitz's view, would drive cyber insurance growth, which would improve compliance through underwriting, again in a way similar to worker's compensation regimes.

As I have discussed in work concerning the economic loss doctrine and data breach claims, the instinct that a private law regime will drive insurance and compliance is important.[295] I continue to believe that the economic loss doctrine should not bar data breach claims where ascertainable economic losses can be proven. I am a bit less sanguine than I was previously, however, about the role of private law in the cybersecurity context.

First, doctrinally and theoretically, as discussed in this paper, the problem of harm is much more difficult than any of the existing literature admits. Hurwitz's idea of "statutorily directed" damages might make it easier for plaintiffs to survive a motion to dismiss—assuming this kind of "statutorily directed" damages afford standing to sue—but it does not address the deeper doctrinal and theoretical problems about harm and causation.[296] Most consumers will not suffer concrete economic losses as a result of commercial data breaches, for the reasons explained in Part I above. It is unclear whether Hurwitz wants to extend "statutorily directed" damages to a schedule of dignitary or emotional harms, but if so, this would contradict

289. One aspect of this problem relates to the complexity of computer software. As Hurwitz has noted, for example, the "halting problem" suggests that "it is effectively impossible to prove that any computer code beyond a trivial level of complexity operates as intended." Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1503 (2017).

290. *Id.* at 1495.

291. *Id.* at 1514–16.

292. *Id.* at 1516–18.

293. *Id.* at 1529.

294. *Id.*

295. *See* Opderbeck, *supra* note 73.

296. Hurwitz, *supra* note 289, at 1529.

sound tort doctrine and theory, as explained in Part II above. Further, as also explained in Section I.C above, tracing any kind of harm to any specific data breach is in most cases impossible. It is difficult to see how Hurwitz's "statutorily directed" harms avoid becoming a kind of general enterprise liability.

In addition, modern strict liability rules in products liability cases are not so "strict" as Hurwitz assumes. Modern strict liability rules in cases involving manufacturing, design, or informational (instruction and warning) defects tend to converge on risk-utility tests that resemble the test for negligence.[297] And strict product liability cases often present difficult questions of causation, along with defenses such as product misuse, "state of the art," obvious or inherent dangers, and so on.[298] A "state of the art" or obvious or inherent danger defense would be potent in the data breach setting, given the hard problem of cybercrime.[299]

My second reason for my greater skepticism about private law remedies as a cybersecurity tool results from empirical work on data breach class actions.[300] Scholars such as Solove and Citron suggest that, even if individual non-economic harms are small, the aggregation function of class actions will help drive systemic compliance and will provide meaningful remedies to consumers.[301] My empirical research shows that the primary benefits offered to consumers in data breach class action settlements, other than reimbursement for demonstrable out-of-pocket losses, are enhanced security measures and a year or two of free identity theft insurance.[302] The enhanced security measures promised by defendants are described, if at all, in documents filed under seal. Given the realities of the hard problem of cybercrime, we can be skeptical about the true value of this supposed benefit in most cases. The free identity theft insurance, as discussed in Section II.C above, is usually not worth much in practice. Perhaps this kind of litigation plays some role in bumping cybersecurity compliance, but the usual criticism

297. *See generally* MICHAEL I. KRAUSS, PRINCIPLES OF PRODUCTS LIABILITY 91–174 (3d ed. 2011); RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY §§ 1–8. For an excellent discussion of the evolution of strict product liability law, comparing the Second and Third Restatement approaches, see Tincher v. Omega Flex, Inc., 104 A.3d 328, 382 (Pa. 2014) (noting that "[a] broad reading of [the Second Restatement of Torts] suggests that liability would attach absolutely, once the consumer or user suffers harm . . . [b]ut, experience has taught otherwise and, in modern application, strict liability doctrine is a substantially narrower theory").

298. *See generally* KRAUSS, *supra* note 297, at 177–252.

299. Given all these caveats, the main advantages to strict liability for plaintiffs over negligence claims, if there are any in a given case, relate to the elimination of a privity requirement between various parties in the chain of production and the plaintiff and various evidentiary burden shifting mechanisms in certain kinds of claims. *See id.* at 15–38, 201–89.

300. Opderbeck, *supra* note 4.

301. Solove & Citron, *Risk and Anxiety*, *supra* note 8, at 781–85.

302. Opderbeck, *supra* note 4.

of class action litigation—that it serves mostly to transfer rents to lawyers—also seems fair.[303] At the very least, the hope that private law could or should play a major role in cybersecurity compliance seems likely to be unrealized without a theory of harm and causation that results in enterprise liability.

B. Data Privacy Laws as Limitations on the Freedom to Contract: The Need for Stronger Regulatory Security Rules

Other scholars argue for regulatory interventions. David Thaw advocates hybrid regulatory models that would combine some "[d]irective" regulation with some "[m]anagement-[b]ased [r]egulatory [d]elegation."[304] In some ways, Thaw's categories reflect the traditional differences between "rules" and "standards."[305] Thaw argues that management-based regulatory delegation, which he characterizes as a standards regime that relates to an organization's size and capabilities and relies heavily on an organization's compliance professionals, should be supplemented by some directive regulation involving specific rules that are applicable across organizations.[306] This argument is broadly consistent with McGeveran's "frameworks" approach, Bambauer's recent emphasis on *per se* standards for obvious violations, and Hurwitz's concept of strict liability for at least some failures, although the place of standards versus rules in Hurwitz's approach is unclear.[307] Thaw, however, focuses entirely on regulatory public law rather than on the private law of torts or contracts.

In contrast to Thaw's more flexible approach, James Cooper and Bruce Kobayashi have argued for a strict liability data security rule in the context of FTC enforcement rather than private tort actions.[308] Like Hurwitz, Cooper and Kobayashi argue that strict liability will facilitate cyber insurance, with

303. *See, e.g.*, Richard A. Nagareda, *Class Actions in the Administrative State: Kalven and Rosenfield Revisited*, 75 U. CHI. L. REV. 603 (2008); Linda S. Mullenix, *Ending Class Actions as We Know Them: Rethinking the American Class Action*, 64 EMORY L.J. 399 (2014); Arthur R. Miller, *The Preservation and Rejuvenation of Aggregate Litigation: A Systematic Imperative*, 64 EMORY L.J. 293 (2014); Howard M. Erichson, *Aggregation as Disempowerment: Red Flags in Class Action Settlements*, 92 NOTRE DAME L. REV. 859, 860 (2016).

304. David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 317 (2014).

305. *See, e.g.*, Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 559–60 (1992).

306. Thaw, *supra* note 304, at 297–99.

307. *See supra* Section III.A.

308. James C. Cooper & Bruce H. Kobayashi, *Unreasonable: A Strict Liability Solution to the FTC's Data Security Problem*, 28 MICH. TECH L. REV. 257 (2022). A similar proposal from Peter Omerod seems to suffer from the same difficulty of conflating a *per se* statutory rule with "strict liability." Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1936–39 (2019); *see also* Peter C. Ormerod, *Making Privacy Injuries Concrete*, 79 WASH. & LEE L. REV. 101, 157–71 (2022) (discussing privacy statutes that in the author's assume an injury in fact and thereby would function akin to strict liability).

the benefits of underwriting and risk spreading.[309] Cooper and Kobayashi's approach to strict liability would avoid the rent-seeking inherent in private class action litigation.[310]

Also, like Hurwitz, Professors Cooper and Kobayashi conflate strict liability with absolute liability. They state that "a strict liability rule does not dictate a level of security. Instead, it works by requiring a firm to pay for all the external harm it causes regardless of the level of care taken."[311] As noted above, this is not how modern strict liability doctrine works, although Cooper and Kobayashi are using this private law concept only analogically in a public law context. Further, the reference here to "harm" begs the fundamental question of whether any individual data security incident causes any identifiable harm to any specific individual. Cooper and Kobayashi suggest that "when there is no evidence of direct harm, the FTC can estimate increased risk of harm from breaches of Personally Identifiable Information (PII) using public and private data from the breached firm."[312] The hard problem of cybercrime and the saturation of PII markets would make this a quixotic endeavor, at best.

Cooper and Kobayashi suggest that there must be individual harms if the cybersecurity problem is an externality problem. The question is one of data and measurement, not one of whether "harm" has occurred.[313] To some extent they are correct, but the externalities of data breaches are far greater than the sum of economic harms to individual consumers. The Internet ecosystem is, by definition, a connected network. Every vulnerable node compromises every other node. An attack on any node requires defensive measures from any other node that wants to resist the attack. The social cost of cybercrime, therefore, includes the sum of actual harms to individuals plus the sum of cyber defense costs throughout the entire network, including the opportunity costs of diverting resources to cyber defense.[314] Although Cooper and Kobayashi are right to suggest the need for some new regulatory rules, the tie to individual harms and a tort-like concept of strict liability is misplaced.

309. Cooper & Kobayashi, *supra* note 308, at 292–96.

310. Of course, as they acknowledge, it would require additional legislative authority for the FTC. *Id.* at 298–99. It would also, of course, raise the usual questions about regulatory capture, agency expertise, and so on.

311. *Id.* at 287.

312. *Id.* at 297.

313. *See id.*; E-mail from James Cooper, Professor of L., Geo. Mason Univ. Antonin Scalia L. Sch., and Bruce Kobayashi, Paige V. & Henry N. Butler Chair in L. & Econ., Geo. Mason Univ. Antonin Scalia L. Sch., to author (Aug. 20, 2022, 5:37 PM EST) (on file with author).

314. I have referred to this as the "network externalities" of cybersecurity. *See* Opderbeck, *supra* note 73, at 960.

Thaw is right, then, to focus on public law, and also right to advocate for a mix of rules and standards.[315] Public law concerning cybersecurity, however, should work in tandem with privacy regulation that changes the terms of private law, specifically concerning the freedom to contract. Comprehensive privacy laws limit the terms on which a data processor or controller can do business with individuals. Such comprehensive privacy laws always address data security, but usually without sufficient emphasis or specificity. One of the most important steps lawmakers can take to support cybersecurity is to embed stronger data security provisions in comprehensive privacy laws.

Contracts complicate privacy "harms" because the contractual terms of service issued by most data controllers and processors severely limit the controller or processor's liability. Google's Terms of Service, for example, disclaims all warranties and purports to limit liability to $200 or the fee paid for services over the preceding 12-month period (which in most cases is $0).[316] Google's Privacy Policy states how Google will process user data, and it identifies Google's security measures, but it does not guarantee against data breaches.[317]

Comprehensive privacy regulation such as the EU GDPR is a mix of contract and tort-adjacent measures. The GDPR regulates both data controllers and data processors.[318] It broadly limits the legal subject matter of contracts between controllers and data subjects by requiring a "lawful basis," as defined in the regulation, for collecting and using PII.[319] It further limits the freedom of data controllers to contract with data subjects by requiring controllers to make certain representations (stating which PII will be processed, why, and how) and to undertake certain obligations (such as the rights of access and erasure) concerning PII of the data subject.[320] For a processor that is not the data controller, the GDPR also limits the freedom to contract between the controller and processor by requiring the processor to take on certain obligations relating to the PII.[321]

315. *See generally* Thaw, *supra* note 304.

316. *See Google Terms of Service*, GOOGLE (Jan. 5, 2022), https://policies.google.com/terms?hl=en-US.

317. *See Google Privacy Policy*, GOOGLE (Dec. 15, 2022), https://policies.google.com/privacy?hl=en-US.

318. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) art. 24–43.

319. *Id.* art. 6.

320. *Id.* art. 24–31.

321. *Id.* art. 28.

Where the controller and processor are not the same entity, the GDPR is a kind of tort-adjacent regulation because the contract between the controller and processor, to which the data subject is not in contractual privity, might impose externalities on the data subject if the processor adopts lower levels of privacy protection than the controller.[322] The GDPR requires the contract between the processor and controller to internalize these costs by imposing privacy obligations on the processor despite the processor's lack of contractual privity with the data subject.[323] In this sense, the GDPR reflects the most salient strict liability themes surfaced by Hurwitz.

The GDPR's security provision, however, is inadequate. Article 32 of the GDPR imposes security requirements on controllers and processors.[324] It refers to a general risk-benefit analysis. The only specific technological requirement is to implement pseudonymization and encryption "as appropriate."[325] Recital 83 of the GDPR states that risk assessments should take "into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected."[326] It further states that "consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage."[327] Again, the only technological measure mentioned in the Recital is encryption.[328] Numerous decisions from national Data Protection Authorities mention Article 32, but this is usually ancillary to other alleged violations, and few of the decisions elaborate on technological or policy measures regarding data security.[329] Article 33 of the GDPR requires controllers to notify the appropriate supervisory authority of any data breaches within seventy-two hours, and Article 34 requires breach notification to individual data subjects "without undue delay."[330]

The U.S. state data privacy laws modeled on the GDPR—which presently include California, Colorado, Virginia, Utah, and Connecticut—

322. *Id.*

323. *Id.*

324. *Id.* art. 32.

325. *See id.* art. 32.1(a). There are three other requirements listed in Article 32.1, but unlike the mention of encryption in Article 32.1(a), they do not refer to any specific technological measure. *Id.* art. 32.1(b)–(d).

326. *Id.* at Recital 83, 2016 O.J. at 16.

327. *Id.*

328. *Id.*

329. See compilation at *Category: Article 32 GDPR*, GDPRHUB (Jan. 12, 2020), https://gdprhub.eu/index.php?title=Category:Article_32_GDPR.

330. Regulation (EU) 2016/679, art. 33, 34, 2016 O.J. (L 119) 1, 52–53.

likewise contain only general data security requirements.[331] The California Consumer Privacy Act ("CCPA") states "[a] business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure."[332] The Virginia, Utah, Colorado, and Connecticut laws are similarly broad and general.[333]

U.S. federal privacy laws in the health care and banking sectors include specific security rules that are better developed than the GDPR or the U.S. state comprehensive privacy laws.[334] The HIPAA Security Rule is one of the most extensive efforts to regulate security standards. The HIPAA Security Rule recognizes the difficulty of establishing a generally applicable standard of care. It states that:

> In deciding which security measures to use, a covered entity or business associate must take into account the following factors:
>
> (i) The size, complexity, and capabilities of the covered entity or business associate.
>
> (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.
>
> (iii) The costs of security measures.

331. For the status of comprehensive state privacy laws, see Anokhy Desai, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Apr. 21, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

332. CAL. CIV. CODE § 1798.100(e) (West 2023).

333. VA. CODE ANN. § 59.1-578.A.3 (2023) (stating that controllers must "[e]stablish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue"); 2022 Conn. Legis. Serv. P.A. 22-15, § 6(a)(3) (West) (stating that controllers must "establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue"); COLO REV. STAT. § 6-1-1308(5) (2023) (stating that controllers must "take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business"); UTAH CODE ANN. § 13-61-302(2) (LexisNexis 2023). The Utah law states that:

> (a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:
>
> (i) protect the confidentiality and integrity of personal data; and
>
> (ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.
>
> (b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

UTAH CODE ANN. § 13-61-302(2) (LexisNexis 2023).

334. For rules relating to banking, see *infra* Section III.C.

> (iv) The probability and criticality of potential risks to electronic protected health information.[335]

At the same time, the HIPAA Security Rule requires all covered entities to engage in regular data security risk analysis, implement specific risk management measures, employ physical safeguards such as access control and validation and technical safeguards such as encryption.[336] As Thaw notes, the HIPAA Security Rule therefore is a hybrid model of standards and rules.[337]

The HIPAA Security Rule provides a good model for privacy-adjacent data security requirements. Its most important feature is perhaps the universal requirement to conduct regular data security risk assessments. The "Identify" function of the NIST Framework requires regular risk assessments and risk management strategies that allow organizations to identify and avoid obvious mistakes and to educate their constituents about risks such as phishing and spoofing.[338] Stronger security rules akin to the HIPAA Security Rule should be incorporated into the GDPR, U.S. state comprehensive privacy laws, and, eventually, a U.S. national comprehensive privacy law.[339]

C. Strengthening the Risk-Spreading Function of the Payment Card System

Absent comprehensive federal legislation, there is one sector-specific intervention that might go further than anything to drive better cybersecurity compliance in an area heavily impacted by commercial data breaches: enhancing the security risk-spreading function of the payment card system. As noted in Section I.C.1, the players in the card payment system adjust this risk among themselves contractually. If a player in the payment card chain suffers a data breach because it has failed to enact the minimum security required by the card network contracts, it will have to pay reimbursement and/or penalties to the other banks in the network. One way or another, one or more of the players—the issuing bank, the acquiring bank, the merchant, and the card brand—will bear the costs of fraud as costs of doing business. These costs will be passed on to consumers in the form of higher fees and/or higher interest rates, which will affect the amount of the overall credit benefit.

335. 45 C.F.R. § 164.306(b)(2) (2023).

336. *Id.* §§ 164.308–312. 45 C.F.R. pt. 164 app. a provides a helpful matrix of required standards under the Rule.

337. Thaw, *supra* note 304, at 327–30.

338. *See* NIST, *supra* note 45, at 23, 26–28.

339. A number of comprehensive data privacy bills are pending in Congress. Many of these bills do not mention data security. Some, including the "Mind Your Own Business Act of 2021" proposed by Senator Ron Wyden, would require the FTC to issue generally applicable data security rules. *See* S. 1444, 117th Cong. § 7(b)(1)(A)–(B) (2021).

All banks and merchants using recognized card brands are contractually obligated to adopt a system of security and compliance measures called the Payment Card Industry Data Security Standard ("PCI DSS").[340] The PCI DSS standard is implemented by the PCI Security Standards Council, an organization established by American Express, Discover, Mastercard, Visa, and JCB International.[341]

Many large merchants provide input into PCI DSS as "participating organization[s]" in the PCI Security Standards Council.[342] Many smaller merchants, however, view PCI DSS as both overly burdensome and ineffective. In 2018, the National Retail Federation, complained to the FTC that "branded card networks under the FTC's jurisdiction are engaged in anticompetitive behavior under the guise of establishing data security standards for other industries that rely on payment cards."[343] The NRF argued that PCI DSS does not satisfy American National Standards Institute ("ANSI") principles for standards development.[344]

Regardless of NRF's antitrust allegations, it seems that most organizations subject to PCI DSS fall short of compliance. The Verizon 2020 Payment Security Report found that only 27.9% of organizations subject to a compliance validation report had achieved full compliance.[345] This finding reflected an almost nine percentage point drop from the prior year.[346] In the 10 years over which Verizon has produced this report, the highest annual rate of full compliance was 55.4% (2016), and the 10-year average was 33.21%.[347] The Verizon Report noted that many organizations had implemented PCI DSS compliance controls that were difficult to sustain over the long term and that the shift to home-based work during the COVID pandemic made compliance particularly difficult.[348] The PCI requirements

340. *See About Us*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ (last visited Apr. 10, 2023).

341. *See id.* JCB International is a Japanese payment card brand. *See* JCB INT'L CREDIT CARD CO., https://www.jcbusa.com/ (last visited Apr. 24, 2023).

342. *See Participating Organization Directory*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/get_involved/participating_organizations (last visited Apr. 24, 2023).

343. Letter from David French, Senior Vice President, Nat'l Retail Found., to Donald Clark, Sec'y, FTC 1–2 (Aug. 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0050-d-0035-155060.pdf [https://web.archive.org/web/20210328012612/https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0050-d-0035-155060.pdf].

344. *Id.* at 8–9.

345. VERIZON, 2020 PAYMENT SECURITY REPORT 6 (2020), https://www.verizon.com/business/resources/Tb43/reports/2020-payment-security-report.pdf.

346. *Id.* at 7.

347. *Id.* at 8.

348. *Id.* at 9–10.

with the least compliance were "test security systems and processes" and "security management."[349]

It is obviously problematic that over the course of ten years, two-thirds of entities subject to contractual PCI DSS requirements were not fully compliant. In the United States, neither the PCI DSS standard nor any other cybersecurity standard is required of merchants by law, apart from security requirements in comprehensive state privacy laws.[350] This gaping regulatory hole should be filled.

In contrast to the lack of regulation for merchants, issuing and acquiring banks are subject to the Graham-Leach-Bliley Act's ("GLBA")[351] data security requirements as well as contractual PCI DSS standards.[352] GLBA's statutory text requires various regulatory agencies the promulgate regulations:

> (1) to insure the security and confidentiality of customer records and information;
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[353]

The agencies responsible for promulgating and enforcing these regulations for banks include the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit Insurance Corporation ("FDIC"), and the Board of Governors of the Federal Reserve System, depending on what kind of bank is involved.[354]

In 2001, the OCC, FDIC, and Federal Reserve, along with other federal agencies, adopted the Interagency Guidelines Establishing Standards for Safeguarding Consumer Information, which were incorporated into agency rules implementing the GLBA security requirement (the "Interagency

349. *Id.* at 64. Test security systems and processes "cover[] the use of vulnerability scanning, penetration testing, file integrity monitoring and intrusion detection to ensure that weaknesses are identified and addressed." *Id.* at 103. Security management "demands that organizations actively manage their data protection responsibilities by establishing, updating and communicating security policies and procedures aligned with the results of regular risk assessments." *Id.* at 108.

350. The exception is for merchants that issue their own payment cards, in which case they are treated as financial services entities under GLBA with respect to those cards and therefore are subject to the GLBA Safeguards Rule. *See* 15 U.S.C. § 6801(b); 12 U.S.C. § 1813(q); 16 C.F.R. § 314 *et seq.* (2023).

351. Graham-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

352. 15 U.S.C. § 6801(b).

353. *Id.*

354. 15 U.S.C. §§ 6804, 6805(b)(1); 12 U.S.C. § 1813(q).

Guidelines").[355] The Interagency Guidelines were amended in 2005 under the Fair Credit Reporting Act, which included additional provisions regarding the proper disposal of customer information.[356] The Interagency Guidelines include a general reasonableness standard and require a written data security plan and regular audits with oversight by the Board of Directors or an appropriate Board committee.[357] Meanwhile, rulemaking and enforcement authority relating to consumer privacy was transferred to the Consumer Financial Protection Board under the Dodd-Frank Act in 2014.[358]

GLBA's data security requirements also fall within the FTC's authority for financial institutions that are subject to the FTC's jurisdiction and are not subject to other regulators under GLBA.[359] The FTC exercises this authority under its GLBA Safeguards Rule.[360] Like the HIPAA Security Rule, the GLBA Safeguards Rule requires the use of encryption, multi-factor authentication, and other standard security measures, along with regular risk assessments.[361] And, like the HIPAA Security Rule, the GLBA Safeguards Rule establishes a general reasonableness standard of compliance that requires covered financial institutions to

> develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.[362]

355. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 12 C.F.R. § 30 app. B (2001).

356. *See* Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003, 69 Fed. Reg. 77,610 (July 1, 2005).

357. *See* Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 12 C.F.R. § 30 app. B. (2001).

358. Dodd–Frank Wall Street Reform and Consumer Protection Act, 15 U.S.C. §§ 6801(a), 6802–6804. For background, see Privacy of Consumer Information, 79 Fed. Reg. 30,708 (May 29, 2014).

359. *FTC Safeguards Rule: What Your Business Needs to Know*, FTC (May 1, 2022), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

360. Banks are "financial institutions" under GLBA and therefore are subject to the Safeguards Rule. *See* 15 U.S.C. § 6801(b); 16 C.F.R. § 314.1(b) (2021).

361. 16 C.F.R. § 314.4.

362. *Id.* § 314.3(a). In the *Equifax* data breach litigation, U.S. District Judge Thomas W. Thrash, Jr. of the Northern District of Georgia granted defendant's Rule 12(b)(6) motion to dismiss a negligence *per se* claim based on the text of the GLBA statute, which Judge Thrash held did not supply a specific standard of conduct that could inform a legal duty. *In re* Equifax Inc. Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1173–74 (N.D. Ga. 2019). This was consistent with the Georgia Supreme Court's holding in *Wells Fargo Bank, N.A. v. Jenkins*, 744 S.E.2d 686 (Ga. 2013), which involved a bank teller who allegedly gave a customer's confidential information to the teller's husband, who stole the customer's identity. However, Judge Thrash denied the motion

The FTC's GLBA Safeguards Rule was originally adopted in 2003, based on the Interagency Guidelines, and was updated in 2021.[363] The amendments include clearer standards on the use of encryption and multi-factor authentication and enhanced requirements for logging, incident response plans, and other protect-defend-respond functions.[364]

It should be obvious that the Interagency Guidelines on cybersecurity adopted in 2001 and last amended in 2005 are due for updating as applied to banks not regulated by the FTC. The FTC's amended Safeguards Rule suggests important ways in which the Interagency Guidelines applicable to banks could be updated, particularly concerning encryption and two-factor authentication. Equally concerning is the fact that enforcement is divided among three different regulators. Even more concerning is the separation of privacy from security—a fundamental mistake—along with the placement of privacy enforcement in yet another agency.[365] All these problems should be rectified.

Three other reforms alongside a stronger, centralized security rule, could help mitigate the worst effects of payment card fraud. First, the statutory fifty-dollar floor for fraud reimbursement should be adjusted to zero. As noted in Section I.C.1, it already is the contractual policy of the major card brands to provide full reimbursement. This is appropriate because the card brands, banks, and merchants are in the best position to implement fraud detection systems and to insure against the costs of fraud. As a merely contractual matter, however, this policy could change at any time. This is unlikely for market reasons as to the four major card brands, but the payment card system is due for disruption as blockchain, cryptocurrencies, and other technologies position different players to make inroads into what for decades

to dismiss as to the GLBA Safeguards Rule, which he held could supply an ascertainable standard. *In re Equifax*, 371 F. Supp. 3d at 1174–75.

363. *See generally* 16 C.F.R. § 314 (2023); FTC, *supra* note 359.

364. *See generally* 16 C.F.R. § 314; Robert Rubenstein, *FTC's Amended Safeguards Rule Imposes Significant Requirements on Covered Entities*, JDSUPRA (Dec. 17, 2021), https://www.jdsupra.com/legalnews/ftc-s-amended-safeguards-rule-imposes-6189469/. The amended Safeguards Rule also purports to expand the entities subject to the FTC's jurisdiction under the Rule. *See* Rubenstein, *supra*. Whether the FTC possesses authority for this change is beyond the scope of this Article.

365. Although data privacy and data security are sometimes considered separate or even competing domains, this perception is incorrect. In cybersecurity circles, it is commonplace to note that while it is possible to achieve data security without privacy, it is not possible to achieve data privacy without security. *See, e.g.*, Alexander Howard & Lorenzo Ligato, *Former DHS Director Chertoff: 'You Can't Have Privacy Without Security'*, HUFFPOST (Oct. 3, 2015, 9:01 AM), https://www.huffpost.com/entry/michael-chertoff-dhs-privacy-security_n_560ebd9de4b076812701c9f7. The convergence of data privacy and cybersecurity will only become more direct in the age of big data analytics. *See* Carl Landwehr et al., *Privacy and Cybersecurity: The Next 100 Years*, 100 PROC. IEEE 1659 (2012), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6182691.

has been an oligopolistic market.[366] Full fraud reimbursement rules should keep the fraud detection onus squarely on both traditional and evolving payment networks rather than on consumers.

Second, federal law should include clear, centralized rules for fraud detection and remediation systems in traditional and evolving payment networks. The Interagency Guidelines include general fraud detection requirements, other banking rules relate to various kinds of bank fraud, and the market supplies fraud detection tools, all of which are good but somewhat unfocused.[367] Perhaps more important than the rules themselves, a centralized regulatory forum should facilitate greater information sharing, standards development, consumer education, and public accountability.[368]

Third, we need a more robust national system for reporting and providing public information about breaches of payment card system information. In one sense, this is yet another call for federal data breach notification and reporting legislation. Such national legislation is long overdue, and ideally should be part of a federal data privacy and security package.[369] Beyond mere notification, the system should include specific reporting mechanisms for payment card breaches, which would enable consumers to securely run checkups on their own card numbers and to obtain reports about breach trends and industry responses. These consumer information functions will help facilitate competition for more secure and responsive payment card networks.

D. Enhanced Responses to the Systemic Risks of True Identity Fraud: Credit Reporting and Social Security Number Reform

A final set of reforms designed to mitigate systemic risk would strengthen consumers' ability to manage the problem of identity theft and transition the Social Security number system into the digital age.

There are presently some good rules around credit reporting that could be enhanced. The Fair and Accurate Credit Transactions Act of 2003

366. *See, e.g.*, Jim McCarthy, *How Crypto-backed Cards are Disrupting Payments*, I2C INC., https://www.i2cinc.com/blog/crypto-cards-disrupting-payments/ (last visited Apr. 24, 2023).

367. *See, e.g.*, AKIF KHAN & DAN AYOUB, GARTNER RSCH., MARKET GUIDE FOR ONLINE FRAUD DETECTION (2022), https://resources.sift.com/ebook/2022-gartner-market-guide-for-online-fraud-detection/ (listing vendors of fraud detection products).

368. Information sharing and a proliferation of uncoordinated regulations is a significant problem for cybersecurity in the U.S. *See* Tim Starks, *Cyber Regulations Proliferate, Creating Fresh Problems*, WASH. POST (July 27, 2022, 7:30 AM), https://www.washingtonpost.com/politics/2022/07/27/cyber-regulations-proliferate-creating-fresh-problems/.

369. There have been numerous privacy bills in Congress in recent years. No comprehensive federal privacy or data breach law has received a floor vote. *See* MÜGE FAZLIOGLU, INT'L ASS'N OF PRIV. PROS., U.S. FEDERAL PRIVACY LEGISLATION TRACKER (2022) https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf.

("FACTA"), as updated in 2010 and 2018, amended the Fair Credit Reporting Act.[370] FACTA presently requires credit reporting agencies to offer one free credit report to the consumer upon request, to place a fraud alert in the consumer's file upon request, to freeze the consumer's credit, and under certain circumstances, to provide additional free reports to the consumer.[371] Consumer reporting agencies must maintain webpages to facilitate these rights, which must be linked by the FTC's "Identitytheft.gov" website.[372] Consumer reporting agencies must also provide active duty members of the military with free electronic credit monitoring notifications.[373]

The FTC issued its "red flags" and "disposal" Rules under FACTA.[374] The "red flags" Rule requires certain financial institutions to establish an identity theft program that must include "reasonable policies and procedure to . . . [i]dentify relevant Red Flags for the covered accounts."[375] "Red Flag" is defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft."[376] The Red Flags Rule also requires credit or debit card issuers to adopt programs to validate cardholder addresses.[377] The Red Flag Rule is accompanied by "Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation."[378] These Guidelines outline the design of red flag detection and remediation programs and list events that should always trigger a red flag warning.[379] The FTC's Disposal Rule, adopted in 2005, requires any entity regulated by the FTC that "maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable

370. 15 U.S.C. § 1681c-1.

371. *Id.* § 1681c-1(a)–(b).

372. *Id.* § 1681c-1(i)(6); *see also* IDENTITYTHEFT.GOV, *supra* note 256.

373. 15 U.S.C. § 1681c-1(k)(2).

374. *See generally Fair and Accurate Credit Transactions Act of 2003*, FTC, https://www.ftc.gov/legal-library/browse/statutes/fair-accurate-credit-transactions-act-2003 (last visited Apr. 24, 2023).

375. 12 C.F.R. § 41.90(d)(2)(i) (2023). The Red Flag Program Clarification Act of 2010 modified the definition of "creditor" in the Rule to exclude entities that extend credit incidental to providing a service to the customer. Red Flag Program Clarification Act of 2010, Pub. L. 111-319, § 2, 124 Stat. 3457, 3457. This amendment came at the behest of healthcare providers and professional service firms. *See, e.g.*, AM. MED. ASS'N, PRAC. MGMT. CTR., PROTECT YOUR PATIENTS, PROTECT YOUR PRACTICE: WHAT YOU NEED TO KNOW ABOUT THE RED FLAGS RULE (2011), https://www.cms.org/uploads/red-flags-rule-edu.pdf.

376. 12 C.F.R. § 41.90(b)(10).

377. *Id.* § 41.91.

378. *Id.* § 41.91 app. J.

379. *Id.* For example, the Guidelines state that a consumer report showing "a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer" should trigger a red flag. *Id.* § 41.91 supp. A to app. J.

measures to protect against unauthorized access to or use of the information in connection with its disposal."[380]

The FTC's Red Flags and Disposal Rules are useful but could be strengthened in several ways. First, instead of merely providing links to the credit agencies' identity theft portals, there should be a national clearinghouse that enables consumers to check all their credit reports and to freeze all their credit with every provider instantaneously through a single source. Through this clearinghouse, consumers should be entitled to unlimited copies of their personal credit reports. Consumers should also have an option to receive automatic alerts through the clearinghouse whenever their credit files are updated.

The build and maintenance of such a system should be considered a piece of national infrastructure designed to protect and enhance the credit benefit.[381] If this cost is financed through a tax on credit agencies, and this cost is passed on to consumers of credit reports this would reflect an acceptable kind of risk spreading and insurance in relation to the value of the credit benefit. The value of the credit benefit, in fact, should increase, and overall costs to consumers should decrease, if the clearinghouse helps mitigate the systemic effects of commercial cybercrime.

Last, the current nine-digit Social Security number should be scrapped in favor of an encrypted digital token secured by two-factor authentication—ideally through biometrics. In the digital age, it is absurd that a stolen nine-digit social security number can do so much mischief without further authentication.[382] Along with enhancements to the payment card system,

380. 16 C.F.R. § 682.3 (2023).

381. As Mark Verstraete and Tal Zarsky suggest, viewing cybersecurity in relation to "infrastructure" highlights the way in which cybersecurity generates spillovers (positive externalities). Mark Verstraete & Tal Zarsky, *Cybersecurity Spillovers*, 47 BYU L. REV. 929, 945 (2022). They advocate strengthening these spillover effects through consideration of spillovers in antitrust policy and through provisions in government contracts. *Id.* at 993–98. Verstraete and Zarsky's argument suggests there that a government subsidy of the clearinghouse proposed here could be warranted. David Vicevich takes the argument about risk spreading a step further and argues for a federal cyber insurance regime. David L. Vicevich, *The Case for a Federal Cyber Insurance Program*, 97 NEB. L. REV. 555, 558 (2018). Something like Vicevich's proposal could complement my call for incremental federal cybersecurity reforms, although his proposal requires greater attention to whether such a federal program would create a moral hazard problem at cross-purposes with regulatory reforms.

382. *See, e.g.*, MCAFEE, MODERNIZING THE SOCIAL SECURITY NUMBER: A FOUNDATION FOR ONLINE AUTHENTICATION OF IDENTITY (2018), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-modernizing-social-security-number.pdf [https://web.archive.org/web/20220815153243/https://www.mcafee.com/enterprise/en-us/assets/reports/rp-modernizing-social-security-number.pdf]. There are, of course, civil liberty concerns inherent in such proposals, including how and for what reasons the government could access something like biometric information connected with a social security identifier. These are important concerns, some of which are similar to existing concerns about social security information and some of which go beyond what is presently on file. These concerns could be addressed in a

these relatively straightforward changes to the credit and Social Security number system would represent significant steps towards managing the systemic risk of commercial cybercrime. These reforms would produce far greater benefits than allowing dignitary, emotional distress, or prophylactic harms in private data breach litigation, without distorting tort or contract law doctrines or transferring more rents to the plaintiffs' class action bar.

CONCLUSION

There is a trend in privacy scholarship emphasizing the dignitary and emotional harms of privacy violations, including the fear of possible future disclosures where information that has been accessed improperly has not been made public. For a wide range of privacy violations, a focus on these kinds of harms might make sense. An act of doxing or sextortion obviously causes real harms even if it causes no physical injuries or financial losses. The focus on dignitary, emotional, and prophylactic remedies, however, is a poor fit in the mine run of commercial data breach cases.[383]

Data processing by commercial entities presents risks, but it is not in itself a harm. The risks of commercial cybercrime are immensely difficult to manage because of the massive scale and sophistication of the cybercrime ecosystem. Cybercrime is a vast global market, connected with organized crime and state actors. A firm that suffers a data breach is the victim of a crime along with any consumers whose PII may have been exfiltrated. Breaches often happen because of failures to implement basic measures such as software patches, but they also happen when the victim is acting reasonably. There is no perfect cybersecurity.[384]

The uses of consumer PII exfiltrated in commercial data breaches vary. In many cases—perhaps in most cases—a specific record containing PII in a given breach is not used in a way that directly economically harms the consumer. The market for consumer PII is saturated. Some of the data is used for credit card fraud, which is quickly reimbursed by the issuing bank. Some of the data is used for synthetic identity fraud, which by definition harms no specific individual. Some is used for true identity fraud, which may or may not result in out-of-pocket costs to the individual. Some may be used for state surveillance purposes that remain opaque to the average person. Much of the stolen consumer PII now available on the dark web is never used for anything at all.[385]

---

variety of ways connected with a requirement for the individual's technological authorization to decrypt certain information. *See, e.g.*, *id.* The details of these questions are beyond the scope of this Article.

383. *See supra* Sections I.C.5, II.B, Part II.

384. *See supra* Section I.A.

385. *See supra* Section I.C.

The average reasonable American consumer in cyberspace, therefore, should not become seriously distressed by a data breach notification. A data breach notification ordinarily requires some prudent awareness rather than panic. Some degree of irritation over data breach notices is part of the price we pay, given the current state of technology, for the numerous benefits of life in cyberspace, including the credit benefit.[386]

As life in cyberspace now stands, data security is a structural problem more than an issue of individual harm. There may be a place for private claims where there is a demonstrable failure to implement easy data security measures resulting in out-of-pocket losses to consumers, but the most productive measures will try to buttress incremental cybersecurity improvements. Data privacy laws, which are essentially limitations on the freedom to contract, should include more robust security provisions. The risk-spreading function of the payment card system should be strengthened by consolidating and updating data security, reporting, and fraud detection processes that are now mixed among contractual PCI DSS norms and various regulatory requirements. Existing regulations around credit reporting should also be updated and consumer rights should be strengthened and brought into a national clearinghouse. Finally, the Social Security number system must be brought into the digital age. These systemic enhancements would help limit the damage done by commercial cybercrime without merely transferring rents to class action lawyers.[387]

386. *See supra* Part II.

387. *See supra* Part III.