Boston College Law Review

Volume 61 | Issue 3 Article 9

3-30-2020

Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation

Max Meglio
Boston College Law School, max.meglio@bc.edu

EMBRACING INSECURITY: HARM REDUCTION THROUGH A NO-FAULT APPROACH TO CONSUMER DATA BREACH LITIGATION

Abstract: The lack of a clear remedy for data subjects whose private information has been compromised in data breaches prompts expensive and exploratory litigation that encounters difficulties with the unique set of risks posed by the data economy. Examining the market forces and risk environments posed by the data economy yields the conclusion that vulnerability is a guaranteed feature and investments in cybersecurity go largely unrewarded. The importance of data to our economy requires that the benefit of potential solutions to data subjects be weighed against the potential costs of burdening innovation. This Note proposes that the ideal solution should prioritize harm reduction by implementing a no-fault resolution system to provide an efficient remedy for compromised data subjects and a safe harbor-based compliance program to improve cybersecurity without hampering the direction of innovation.

INTRODUCTION: OUR BEAST OF BURDEN

If you have ever owned a credit card or had a credit score, your personal data is likely to have been compromised in one or more recent data breaches.[1] A deluge of litigation typically follows in the wake of high profile data breaches as compromised individuals, or "data subjects," seek satisfaction under various tort, contract, and statutory causes of action, generally alleging that the breached entity failed to take sufficient precautions to prevent the breach.[2] The lack of comprehensive federal regulation on the use of consumer data has led to a le-

[1] *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/9FPC-UJ6T] (stating that the Equifax breach alone has compromised the data of essentially every American with a credit report).

[2] *See* Melissa Maleske, *The 6 Lawsuits All GCs Face After a Data Breach*, LAW360 (Dec. 9, 2015), https://www.law360.com/articles/735838 [https://perma.cc/L7K9-ABNV] (reviewing the typical set of lawsuits that companies face in the aftermath of a data breach from consumers, financial institutions, insurers, shareholders, employees, and government entities); *see, e.g.*, Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement at 2–6, *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2017 WL 3699869 (N.D. Cal. June 23, 2017) (chronicling the consolidated litigation comprising over one hundred filed suits and several hundred claims arising out of the laws of all fifty states and the ensuing settlement negotiations). Data subjects are the people whose personal data is collected and used by various entities and comprise consumers, employees, and business clients who must submit to this data collection for functional or commercial purposes. *See* 5 C.F.R. § 293.102 (2020) (defining the term data subject as the individual about whom records are being kept for Office of Personnel Management purposes).

gal vacuum that has been slowly pressurized over years of litigation, enforcement actions, and state regulations, but is still rife with uncertainty.[3] The search for a workable set of legal standards has been stymied by the complexity of technology and the difficulties inherent in data security—to date, no data breach consumer class action suit has made it to trial and litigation of these issues would pose significant challenges.[4] Further complicating a resolution is the recognition that the extension of liability has the potential to shape the direction of innovation and cause shocks to the economy.[5]

The modern economy is heavily dependent on the use of consumer data, but this carries a pervasive risk of identity theft to all data subjects.[6] The amount of leaked personally identifiable information (PII) has increased year-over-year and over eleven thousand breaches have been reported since 2005 comprising over 1.6 billion records.[7] Industry professionals are often hyperbol-

---

[3] *See* Shawn Marie Boyne, *Data Protection in the United States*, 66 AM. J. COMP. L. 299, 302–04, 332–33 (2018) (discussing how the sectoral approach and lack of overarching federal legislation regarding data protection and privacy has created a "latticework of narrowly tailored laws" and remedies).

[4] *See id.* (discussing the varied remedies prescribed by the relevant statutes for each industry). *See generally* 1 E-COMMERCE AND INTERNET LAW § 2.01, Westlaw (database updated Jan. 2020) (providing a background on the development of legal standards to govern data breaches and the significant uncertainty that remains).

[5] *See, e.g.*, Longenecker-Wells v. BeneCard Servs., Inc., No. 1:15-CV-00422, 2015 WL 5576753, at *6 (M.D. Pa. Sept. 22, 2015) *aff'd*, 658 Fed. App'x 659 (3d Cir. 2016) ("[T]he threat of data breaches by unknown third parties is omnipresent[;] . . . the potential disparity between the degree of a defendant's fault and the damages to be recovered could be immensely disproportionate, resulting in drastic implications for defendants . . . as well as our economic system at large."); Brief of the Chamber of Commerce of the United States as Amicus Curiae in Support of Appellees at 21–25, Attias v. CareFirst, Inc., 863 F.3d 620 (D.C. Cir. 2017) (No. 16-7108) (representing business interests as an amicus and arguing that granting standing to plaintiffs who have not yet suffered harm will be costly and burdensome to American businesses); *see also* Thomas J. Kneisner & John D. Leeth, *Regulating Occupational and Product Risks*, *in* HANDBOOK OF THE ECONOMICS OF RISK AND UNCERTAINTY 493, 494, 503 (Mark J. Machina & W. Kip Viscusi eds., 2014) (discussing the effects of liability and policy on innovation); Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1346–50, 1381–83 (2004) (exploring how litigation and legislation assigning liability in novel cyberlaw cases can suppress or shift the direction of innovation, including the "loss of the p2p dissemination network").

[6] *See* N.Y. CYBER TASK FORCE, COLUMBIA SCH. OF INT'L & PUB. AFFAIRS, BUILDING A DEFENSIBLE CYBERSPACE: REPORT OF THE NEW YORK CYBER TASK FORCE 6–9 (2017) (discussing the risks inherent to widespread usage and rapid development of internet technologies); Paul E. Black, *A Software Assurance Reference Dataset: Thousands of Programs with Known Bugs*, 123 J. RES. NAT'L INST. STANDARDS & TECH., 2018, at 1, 1–3 (describing the Software Assurance Reference Dataset, a collection of over one-hundred seventy thousand known software bugs, and explaining how code of typical industry quality tends to contain readily identifiable bugs that are sometimes basic weaknesses made more complicated by the specific code complexities implemented); *Data Is Giving Rise to a New Economy*, THE ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy [https://perma.cc/T4F3-M5GJ] (emphasizing the importance of data to our economy).

[7] *See Data Breaches*, IDENTITY THEFT RESOURCE CTR., https://www.idtheftcenter.org/data-breaches/ [https://perma.cc/VE83-K52Z] (compiling reported breach figures since 2005); *ITRC Multi-*

ic in their characterizations of how difficult data security is and how consumers should regard data breach as an inevitability.[8] Additionally, organizations are incentivized to invest as little as they can get away with in cybersecurity as the return on these proactive investments tends to be low and damage control is often cheaper and likely to be incurred anyway.[9]

Data breaches create substantial costs for both the compromised individuals who face the risk of identity theft as well as breached organizations who must answer to angry data subjects, shareholders, regulators, or other stakeholders.[10] Much of the harm to data subjects comes in the form of poorly understood increased future risks, complicating projections of what actual costs flow from a data breach and who bears them.[11] The uncertain regulatory land-

---

Year Data Breach Chart Jan. 1, 2005–Dec. 31, 2018, IDENTITY THEFT RESOURCE CTR., https://www.idtheftcenter.org/wp-content/uploads/2019/02/Multi-Year-Chart.pdf [https://perma.cc/9F6S-4R3X] (graphing the increase from 157 reported breaches in 2005 to over one thousand reported breaches in each of the past three years). Privacy Rights Clearinghouse tallies a drastically higher number: over eleven billion records breached since 2005. *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches [https://perma.cc/GZ8J-PRGE]. Generally, personally identifiable information (PII) is that which could be used to identify a particular data subject. *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: Protecting Consumer Privacy in the Digital Age, 3–4 (Aug. 22, 2016), https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_n_digital_age_aspen_8-22-16.pdf [https://perma.cc/XMG9-P6H7]. As data collection becomes more sophisticated, some at the Federal Trade Commission (FTC) have advocated for an expansion of the traditional categories of PII to include other more abstract types of data such as static Internet Protocol addresses that can be used to track down data subjects despite lacking clear identifiers. *See id.* (discussing how sophisticated analyses of meta-data have expanded the usefulness and ability to attribute data that lacks personal identifiers).

[8] *See, e.g.*, BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY 19 (2018) ("The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards—and even then I have my doubts.") (quoting expert Gene Spafford); *see also* N.Y. CYBER TASK FORCE, *supra* note 6, at 6–9 (discussing the architectural and human reasons why cybersecurity struggles to keep up with attackers).

[9] *See* Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 220–22 (2017) (explaining how the risks and incentives for internet-connected products sometimes favor cheap design over security); Jun Zhuang et al., *Subsidies in Interdependent Security with Heterogeneous Discount Rates*, 52 ENGINEERING ECONOMIST 1, 16–18 (2007) (modeling a dominant strategy of low investment in security when there are high investment costs and factors that diminish the return on investment); Bruce Schneier, *Liability Changes Everything*, SCHNEIER ON SECURITY (Nov. 2003), https://www.schneier.com/essays/archives/2003/11/liability_changes_ev.html [https://perma.cc/A4JQ-XY42] (describing the costs of cybersecurity compared to damage control and how it produces a rational financial decision to invest as little as possible into cybersecurity).

[10] *See* PONEMON INST., 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 15 (2018) (finding that data breaches cost American companies an average of $7.91 million); Maleske, *supra* note 2 (describing the six classes of stakeholders who are likely to be plaintiffs in data breach litigation).

[11] *See* PAUL DREYER ET AL., RAND CORP., ESTIMATING THE GLOBAL COST OF CYBER RISK 1 (2018) (explaining that the costs created by exfiltration of PII are difficult to model due to complex second-order costs); IDENTITY THEFT RESOURCE CTR., IDENTITY THEFT: THE AFTERMATH 2017, at 7 (2018) [hereinafter THE AFTERMATH 2017] (listing a variety of negative effects of identity theft); *Attor-*

scape and lack of a clear consumer remedy create an inefficient response to this ubiquitous threat by prompting complex litigation actions and unclear compliance obligations that substantially add to overall costs.[12]

This Note argues that a no-fault scheme including a centralized consumer remedy and a safe harbor-based regulatory program with clear compliance standards would reduce the costs that flow from the inevitable breaches without stifling innovation.[13] Part I of this Note provides an overview of the costs created by data breaches and the scope of data breach litigation.[14] Part II presents some of the market characteristics that have frustrated the development of robust data security practices and discusses the difficulty of regulating internet technologies due to the possible chilling effects on innovation.[15] Part III argues that a limited harm reduction framework can better account for the importance of data to our economy, the inevitability of data insecurity, and the difficulty of creating legal and technical standards than traditional approaches to private liability.[16] Additionally, the safe harbor incentive and clearer compliance costs will more effectively encourage sustainable security practices than the current uncertain standards that reward reactive damage control rather than proactive investment into security.[17]

---

ney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, DEP'T OF JUSTICE (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military [https://perma.cc/MJ3W-2778] (detailing the potentially wide ranging harms that may flow from the Equifax breach, which has now been attributed to the Chinese military).

[12] *See* PONEMON INST., *supra* note 10, at 28 (reporting that data breaches cost American organizations an average of $1.76 million in post-breach response expenses including litigation and regulatory intervention costs).

[13] *See infra* notes 134–200 and accompanying text (discussing the market failures and environment of risks that are stifling the development of legal standards and the excess costs they create); *infra* notes 201–272 and accompanying text (analyzing the greater efficiency of a no-fault approach).

[14] *See infra* notes 18–133 and accompanying text (providing background information on the costs that data breaches cause to both data subjects and organizations and on data breach litigation).

[15] *See infra* notes 134–200 and accompanying text (discussing the issues preventing effective cybersecurity and the implications that imposing new standards may have on innovation).

[16] *See infra* notes 201–272 and accompanying text (analyzing the issue and proposing a solution). *See generally* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236–37 (11th Cir. 2018) (discussing the difficulty of developing reasonable security standards); Stephen Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357, 358–64 (1984) (discussing the determinants of when government intervention may benefit the social welfare).

[17] *See* Mark. A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. ON TELECOMM. & HIGH TECH. L. 101, 110–13, 119 (2007) (analyzing several safe harbor regimes and concluding, despite any imperfections, that "[i]nternet intermediaries need safe harbors"); *see also infra* notes 239–272 and accompanying text (explaining the merits of this approach within this context).

I. YOU CAN'T ALWAYS GET WHAT YOU WANT: A CRASH COURSE IN DATA BREACH LITIGATION

The impact of data integration on our modern economy has been likened to the effect of oil on the industrial revolution.[18] Data augments and improves existing operations and gives rise to an entire industry of data services and information technology enterprise solutions.[19] The growing usage of data has also created a thriving black market for this information and large datasets are now profitable targets for cybercriminals.[20]

This Part will provide a brief overview of data breaches, the costs they create, and the types of litigation and enforcement actions that tend to follow them.[21] Section A explores the costs that flow from data breaches to data subjects and breached entities.[22] Section B provides a summary of the varied litigation and enforcement actions that data breaches prompt.[23]

A. The Cost of Data Breach

Data breaches create substantial costs that are borne by data subjects, the breached entity, and other third-parties.[24] Data breaches comprise several types of incidents that result in the exposure of data, including: malicious cyberattacks, attacks targeting human employees, and even inadvertent errors.[25] The

---

[18] *See Data Is Giving Rise to a New Economy*, *supra* note 6 (analogizing the effect of data as a driver of growth to the effect of oil on the industrial revolution). Taking it a step further, *The Economist* has even suggested data has supplanted oil as the world's most valuable resource. *See The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/4KV5-7EP4] (discussing the value of data to the modern economy).

[19] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 51–53 (2015) (discussing the feedback loop created by the usage of data that has influenced the growth of the data broker industry, which in turn affects marketing and strategy in many other industries).

[20] *See* JAMES ANDREW LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, ECONOMIC IMPACT OF CYBERCRIME: NO SLOWING DOWN 2–6 (2018) (linking the growth of cybercrime to growing internet usage and new ways to monetize this personal information).

[21] *See infra* notes 24–126 and accompanying text.

[22] *See infra* notes 24–63 and accompanying text.

[23] *See infra* notes 64–126 and accompanying text.

[24] *See* N. ERIC WEISS & RENA S. MILLER, CONG. RESEARCH SERV., R43496, THE TARGET AND OTHER FINANCIAL DATA BREACHES: FREQUENTLY ASKED QUESTIONS 14–19 (2015) (listing the costs of payment card data breaches unique to each of the various stakeholders); DREYER ET AL., *supra* note 11, at 4–9 (modeling the costs of cyber risk); PONEMON INST., *supra* note 10, at 3 (listing findings on the average total cost of a data breach). Various sources attempt to put an average monetary value on each record compromised, but the wealth of variables involved in each case limits the cost-predictive use of these without more specific knowledge of what data an entity possesses. *See, e.g.*, PONEMON INST., *supra* note 10, at 7–8 (detailing various factors found to affect the cost of a given data breach).

[25] *See* PONEMON INST., *supra* note 10, at 8 (identifying the three main classes of data breach as malicious attacks, computer glitches, and human error).

internet has grown exponentially, but also incrementally, yielding a system comprised of a patchwork of proprietary software, networks, and protocols layered tenuously on top of one another.[26] The same architecture that makes it so accessible to innovators and users also makes security a virtual impossibility and leaves us with a tangled network of known and unknown vulnerabilities as well as a pervasive threat of data breach.[27] The complexity of technology also makes the average user highly vulnerable to phishing and social engineering.[28]

The disclosure by Marriott International that the data of up to 383 million people had been compromised adds to the list of highly publicized mega-leaks that have afflicted companies like Yahoo (500 million sensitive records) or Equifax (143 million Social Security Numbers (SSNs)).[29] Several ignominious

---

[26] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 7 (explaining how software is designed for accessibility and compatibility with many other programs and devices and how this lack of uniformity undermines cybersecurity); SCHNEIER, *supra* note 19, at 140–43 (discussing the complexity of our computer systems).

[27] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 4–9 (discussing the inherent challenges of securing complex and varied networks); SCHNEIER, *supra* note 19, at 141 ("Complexity is the worst enemy of security, and our systems are getting more complex all the time."); Black, *supra* note 6, at 1–4 (detailing the SARD dataset of over 170,000 known software bugs). This complexity creates vulnerabilities, but also greatly complicates forensic analysis and challenges experts who seek to understand how a given breach occurred. *See* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 54 (2018) (detailing the testimony of the forensic analysts investigating the Equifax breach and the difficulty they encountered due to the "very complex" technology infrastructure in place with multiple outdated legacy systems adapted to function alongside newer systems). Additionally, cybersecurity improvements can sometimes backfire and increase vulnerability by introducing further complexity to computer systems. *See* Josephine Wolff, *Perverse Effects in Defense of Computer Systems: When More Is Less*, 33 J. MGMT. INFO. SYS. 597, 599 (2016) (discussing how unforeseen interactions between security measures and system components can give rise to unexpected vulnerabilities).

[28] *See* IDENTITY THEFT RES. CTR., PHISHING AND TAX FRAUD: UNDERSTANDING THESE GROWING CRIMES' EFFECTS ON BUSINESSES 1–2 (2017) (discussing the sophistication and effectiveness of human-targeted cybercrimes that seek to exploit the lack of knowledge of lay employees of businesses).

[29] *See* Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/824C-BASU] (reporting on the scope of the Yahoo breaches); *2017 Cybersecurity Incident*, EQUIFAX, https://www.equifaxsecurity2017.com/ [https://perma.cc/PF4A-XWV5] (providing information about the Equifax leak and affected consumers); *Marriott Provides Update on Starwood Database Security Incident*, MARRIOTT INT'L: NEWS CTR, (Jan. 4, 2019), https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/ [https://perma.cc/RDW7-QTQU] (providing the updated results of internal investigations into the scope of the breach); *see also* S.C. DEP'T OF REVENUE, PUBLIC INCIDENT RESPONSE REPORT 2–4 (2012) (detailing the findings of the investigation into the hack of South Carolina taxpayer data); *What Happened*, OFFICE OF PERS. MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [https://perma.cc/D34S-GQT4] (providing information about the Office of Personnel Management breaches that compromised over 21.5 million Social Security Numbers). The Marriott breach has been attributed to Marriott's acquisition of the Starwood brand of hotels and the continuous exploitation of a vulnerability in the Starwood reservation system apparently dating back to 2014. *Marriott Provides Update on*

websites track the daily disclosure of breaches in both the public and private sector.[30] One organization tallied that over 446 million records containing sensitive PII were compromised in 2018.[31]

1. Data Subject Harms: Identity Theft and Elevated Lifetime Risk

In 2014, the Bureau of Justice Statistics estimated that 7% of all U.S. residents age sixteen or older had been victimized by identity theft over the prior year, with this number rising to 10% in 2016.[32] Fraudulent charges are the most concrete identity theft harm, but a number of more abstract harms have been noted as well.[33] In many cases, the charges are reimbursed by some intermediary and estimates vary on how often victims are forced to bear these costs.[34] One 2016 report estimated that only 12% of victims faced out of pocket losses, but a recent survey found that almost 40% of respondents were in

Starwood Database Security Incident, *supra* (discussing how the acquisition of Starwood and its vulnerable systems led to the Marriott data breach despite Marriott's cybersecurity efforts).

[30] *See, e.g.*, MASS. OFFICE OF THE ATT'Y GEN., DATA BREACH NOTIFICATION REPORT 2018, at 1–90 (2019) (providing Massachusetts data breach disclosures); *Breach Portal*, OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [https://perma.cc/683W-QQPJ] (showing the Health and Human Services HIPAA violation breach page); *Data Breach Notifications*, WASH. STATE OFFICE OF THE ATT'Y GEN., http://www.atg.wa.gov/data-breach-notifications [https://www.atg.wa.gov/data-breach-notifications] (providing Washington data breach disclosures); *Search Data Security Breaches*, CAL. OFFICE OF THE ATT'Y GEN., https://oag.ca.gov/privacy/databreach/list [https://perma.cc/7KF9-KVU7] (providing California data breach disclosures); *see also* IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT 7 (2019) (reporting that over 2,300 government agencies across thirty-five states were impacted by the breaches of two third-party payment platforms); *News Sections*, DATABREACHES, https://www.databreaches.net/ [https://perma.cc/MU9L-YFBM] (providing an updated-daily-tracker of breaches large and small).

[31] *See* IDENTITY THEFT RES. CTR., *supra* note 30, at 9 (tallying numbers from reported breaches). The report contains a disclaimer that these figures are only based on what is reported and notes that many breaches are likely as-yet undetected or unreported. *Id.* Only half of the 1,244 reported breaches also reported the number of records compromised and the 446 million records represent only those that reported those figures. *Id.*

[32] ERIKA HARRELL, BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2016, at 2 (2019) [hereinafter HARRELL, VICTIMS OF IDENTITY THEFT, 2016]; ERIKA HARRELL, BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2014, at 2 (rev. 2017) [hereinafter HARRELL, VICTIMS OF IDENTITY THEFT, 2014].

[33] *See* IDENTITY THEFT RES. CTR., THE AFTERMATH: THE NON-ECONOMIC IMPACTS OF IDENTITY THEFT 2018, at 1, 3–4, 7–8 (2018) [hereinafter THE AFTERMATH 2018] (finding that victims of identity theft report negative impacts spanning mental, physical, and interpersonal issues); THE AFTERMATH 2017, *supra* note 11, at 7–12 (finding many negative financial impacts caused by fraudulent charges as well as negative emotional and physical impacts).

[34] *See* 15 U.S.C. § 1643 (2018) (limiting consumer liability for fraudulent charges if card issuers provide proper notification channels); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 696–97 (7th Cir. 2015) (discussing scenarios where certain reimbursement policies may be foreclosed by delays in reporting fraudulent charges); 12 C.F.R. § 205.6 (2020) (limiting consumer liability for fraudulent charges if the charges are reported in a timely fashion).

debt or struggling to pay their bills after identity theft.[35] Another survey showed considerable consumer dissatisfaction with how resolution processes are handled, reporting satisfaction levels under 50% for what are sometimes protracted dealings with financial institutions, credit agencies, law enforcement, and federal regulators.[36]

The harm of identity theft also relates to what data is stolen—consumers who have different information stolen face different risks and over different time periods.[37] Stolen credit card information is a short term risk to consumers because the cards are easily canceled and the damage is generally limited to the fraudulent charges that a thief can incur before being detected.[38] SSNs are not as easily replaced and, when leaked, can create a potential lifetime of vulnerabilities.[39] In 2017, almost 158 million SSNs were exposed across 1,579 tracked breaches.[40] The Equifax breach alone exposed a reported 145.5 million SSNs.[41]

There are additional identity theft harms that are harder to quantify, such as the increased risk of future fraudulent activity and the varied emotional harms of compromised privacy.[42] There also may be new harms that material-

---

[35] *See* HARRELL, VICTIMS OF IDENTITY THEFT, 2016, *supra* note 32, at 9 (finding that 12% of victims faced out of pocket costs); IDENTITY THEFT RESOURCE CTR., *supra* note 11, at 8 (finding that almost 40% of respondents experienced financial difficulties of some kind). Over 30% of consumers reported that they borrowed money or took out loans as a result of their identity theft and 15% sold property to pay expenses. IDENTITY THEFT RESOURCE CTR., *supra* note 11, at 8. Mitigating the harm of an incident often requires consumers to take time off work or away from family, close accounts, or even move residences. *Id.*

[36] *See* THE AFTERMATH 2018, *supra* note 33, at 5 (reporting satisfaction levels under 50% for consumer dealings with credit issuers and financial services, credit reporting agencies, law enforcement, and the FTC); *see also* THE AFTERMATH 2017, *supra* note 11, at 13 (finding that over 60% of respondents had yet to resolve their identity theft issues and that 10% of them had spent from one to five years attempting to do so).

[37] *See* HARRELL, VICTIMS OF IDENTITY THEFT, 2016, *supra* note 32, at 9, 11 (showing that the type of identity theft has an impact on the time required to resolve and both the financial and emotional harms reported).

[38] *See* IDENTITY THEFT RES. CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW 5 (2018) (labeling SSN's as the most valuable piece of data to thieves); Stan Horaczek, *Your Social Security Number Probably Got Leaked and That's Very, Very Bad*, POPULAR SCI. (May 10, 2018), https://www.popsci.com/social-security-number-equifax-leak [https://perma.cc/K7TS-K7ER] (remarking on the lesser threat that credit card information theft poses compared to social security number theft).

[39] *See* Horaczek, *supra* note 38 (reporting on the long-term threat of leaked Social Security Numbers and the difficult, long, and expensive process to get a new one). Stolen Social Security numbers empower bad actors to open lines of credit, new accounts, and file false tax returns among other nefarious acts. *See id.*

[40] IDENTITY THEFT RES. CTR., *supra* note 38, at 5.

[41] *See* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 53 (2018).

[42] *See Remijas*, 794 F.3d at 692–93 (reasoning that the heightened risk of future injury sufficed for standing even before actual injury occurred, and asking, "Why else would hackers . . . steal consumers' private information?"); IDENTITY THEFT RES. CTR., *supra* note 11, at 7 (listing a variety of

ize in the future.[43] Experts had been puzzled over the seeming lack of traditional criminal activity associated with the Equifax data and suspected this might indicate more nefarious uses, including blackmail of potential intelligence assets and other statecraft.[44] The Department of Justice's recent issuance of indictments against four Chinese military hackers, alleging their responsibility for the Equifax hack at the direction of the Chinese intelligence services, indicates that the threat posed by this massive theft of data could be equally massive in scope.[45]

2. Organizational Harms

Data breaches cause organizations to experience a mix of quantifiable harms, like breach response and litigation costs, as well as harder to quantify harms like reputational damage.[46] In 2018, the average total cost of a data breach to an American organization was estimated at $7.91 million or $233 per record.[47] Data breaches include both inadvertent mistakes that leave data exposed to potential misuse as well as the costlier malicious cyberattacks, where

---

negative effects of identity theft); IDENTITY THEFT RES. CTR., *supra* note 33, at 3, 5 (noting that victims experience a variety of life impacts and emotional disruptions).

[43] *See* SCHNEIER, *supra* note 8, at 50–51 (describing the "identity theft of the future" as "scary" in part because we cannot yet predict what authentication and identification issues may emerge); *see also* PATRICK O'REILLY ET AL., NAT'L INST. STANDARDS & TECH., 2017 ANNUAL REPORT: NIST/ITL CYBERSECURITY PROGRAM 1 (2018) (noting that advances in quantum computing could result in widespread vulnerability by rendering current encryption standards obsolete). Schneier poses a terrifying hypothetical: data-based assassinations. SCHNEIER, *supra* note 8, at 79. He worries about a future in which hackers can modify medical data to set a target up to receive a transfusion with the wrong blood type or a medicine that they are allergic to, as well as other similarly dystopian uses. *See id.*

[44] *See* Kate Fazzini, *Equifax Mystery: Where Is the Data?*, CNBC (Feb. 13, 2019), https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html [https://perma.cc/FDG4-FBMC] (reporting on the concerns of security experts, who had not been able to locate the Equifax data for sale on the dark web for use in typical identity theft schemes in the immediate aftermath of the breach).

[45] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, *supra* note 11 (announcing the results of a two year investigation into the source of the Equifax breach and the ensuing indictment of four hackers associated with the Chinese military). Attorney General Barr's remarks reflected a high degree of confidence in the attribution of this breach to these hackers. *See id.* He commented that although issuing indictments against the members of foreign militaries is irregular, the seriousness of the breach and the potential scope of the harm to both American consumers and businesses "cannot be countenanced." *Id.*

[46] *See* PONEMON INST., *supra* note 10, at 30 (comparing the "direct and indirect costs" that follow data breaches and how they differ across countries and industries). Stringently regulated industries, such as financial services and healthcare, face higher average costs, likely a result of the types and amounts of data those industries tend to collect and the increased regulatory burden following a breach. *See id.* at 18 (finding higher costs in the healthcare and financial services industries).

[47] *Id.* at 9. The United States led all countries in both average total cost as well as average per capita costs, per record compromised. *Id.*

data is targeted by bad actors and exfiltrated.[48] The risk posed by a potential data breach prompts substantial investment into cybersecurity in order to mitigate these costs or avoid them altogether.[49]

The moment an organization discovers a breach, the clock starts on a handful of regulatory requirements that all require careful navigation.[50] Immediately following the breach, many organizations conduct investigations, engage forensic and communications firms, and implement damage control techniques that are designed to limit some of the long term costs.[51] Breach incident response firms are often brought in, at considerable expense, to oversee the investigation and notification process in order to minimize exposure to liability as a result of the breach.[52] Loss of productivity often results as efforts are shifted organizationally to address the breach.[53] In the longer term, organizations suffer reputational harms, loss of goodwill, and customer loss that vary by industry and the availability of alternatives.[54]

Organizations face significant costs from data breach litigation due to the volume and complexity of the suits likely to be filed.[55] Simply projecting the

---

[48] *See id.* (finding that most breaches are caused by targeted attacks and that these attacks cost organizations more per compromised record than other types of data breach). In some cases, inadvertent exposures are discovered internally and rectified before they are discovered by bad actors, which may account for why these categories yielded lower average costs per capita. *See id.* at 8–9.

[49] *See* COUNCIL OF INS. AGENTS & BROKERS, CYBER INSURANCE MARKET WATCH SURVEY: EXECUTIVE SUMMARY, FEBRUARY 2019, at 2–3 (2019) (finding that 33% of respondents had purchased some type of cyber insurance for the first time in the past year, a figure consistent with previous years); Guarav Pendse, *Cybersecurity: Industry Report & Investment Case*, NASDAQ (June 25, 2018), https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html [https://perma.cc/Q2JZ-6B9X] (discussing how the increasing number of cyber-incidents are contributing to the expansion of the cybersecurity industry).

[50] PONEMON INST., *supra* note 10, at 22 (comparing the effect of twenty-two different preparedness and incident response techniques on the average costs of data breach); *see, e.g.*, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Exchange Act Release No. 10,459, 118 SEC Docket 3993 (Feb. 21, 2018), 2018 WL 993646, at *7–13 (providing guidance on cybersecurity disclosure obligations for public companies that experience incidents).

[51] *See* DREYER ET AL., *supra* note 11, at 1 (finding that immediate mitigation costs account for 10% of total breach costs and less immediate mitigation costs account for another 8% of the total); PONEMON INST., *supra* note 10, at 22 (finding that retention of an incident response team produces the greatest cost savings of all twenty-two preparedness and response factors).

[52] *See* PONEMON INST., *supra* note 10, at 22 (showing that retaining a breach response firm produces a positive return on investment by reducing the costs of the breach).

[53] *See* IDENTITY THEFT RES. CTR., *supra* note 28, at 1 (noting that the resolution of phishing attacks was found to cost an average of over $1.8 million in lost productivity); PONEMON INST., 2017 COST OF CYBER CRIME STUDY 29 (2017) (finding that business disruptions, including lower employee productivity, accounted for almost one-third of the cost consequences of a cybercrime).

[54] *See* DREYER ET AL., *supra* note 11, at 1 (finding reputational losses made up 8% of costs in an aggregated data set of breaches); PONEMON INST., *supra* note 10, at 29 (finding that American organizations face higher costs due to customer churn and loss of goodwill than other countries).

[55] *See* Maleske, *supra* note 2 (discussing the various data breach litigation actions that breached organizations are likely to face); *see, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1172–76 (D. Minn. 2014) (analyzing complex issues of class representation, state

various regulatory stakeholders and potential plaintiffs is a difficult task and requires knowledge of what data was taken and the technical aspects of the intrusion.[56] Settlements with compromised data subjects generally include provisions establishing reimbursement funds and credit monitoring services.[57] Shareholder derivative suits allege breaches of fiduciary duty or inadequate public risk disclosures.[58] Regulators may seek fines and stakeholders are likely to seek enhanced disclosure obligations and future audits as part of probationary compliance plans.[59]

---

causes of action, and state common laws in a consolidated set of thirty-three actions originally filed in eighteen districts); Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 1–6 (detailing the scale of the two-year litigation that included over two hundred depositions, fourteen discovery motions, and 3.8 million pages of documents despite being limited as a streamlined bellwether trial testing only certain claims).

[56] *See, e.g.*, Second Amended Class Action Complaint for Violations of the Federal Securities Law at 2, 4–8, *In re* Yahoo! Inc. Sec. Litig., No. 17-CV-00373-LHK, 2018 WL 4283377 (N.D. Cal. Sept. 7, 2018) (alleging that a class of shareholders of Yahoo stock were harmed by failures to safeguard data and then properly disclose the breach); *Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/WS7N-NJTY] (listing state breach notification statutes); *see also* 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), art. 33, 2016 O.J. (L 119/1) (creating breach disclosure obligations for entities in possession of PII of residents of the European Union); Martin F. Grace, *Economics of State Versus Federal Regulation*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF INSURANCE LAW 321, 328–29 (2015) (explaining the extra costs inherent to compliance with multiple regulatory schemes).

[57] *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 318 (N.D. Cal. Aug. 15, 2018) (discussing the $115 million settlement, including $15 million set aside as a general out-of-pocket-cost reimbursement fund and two years of credit monitoring for affected individuals); *Home Depot Breach Settlement*, KCC CLASS ACTION SERVS. LLC, http://www.homedepotbreachsettlement.com/ [https://perma.cc/CFM8-QZ3A] (providing a claim form entitling class members to reimbursement from the $13 million settlement fund and free credit monitoring for eighteen months under settlement terms).

[58] *See* Maleske, *supra* note 2 (discussing shareholder derivative lawsuits following data breaches); *see, e.g.*, Second Amended Class Action Complaint for Violations of the Federal Securities Laws, *supra* note 56, at 2, 7–8 (alleging that a class of shareholders of Yahoo were harmed by failures to safeguard data and then properly disclosed the breach).

[59] *See, e.g.*, Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 7 (listing Anthem's three-year auditing and reporting obligations to the plaintiff class of consumers); FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017, at 4–5 (2018) (listing significant FTC enforcement actions for data security violations in 2017); Resolution Agreement between Anthem, Inc. and Dep't of Health and Human Servs. 2–3 (Oct. 15, 2018), https://www.hhs.gov/sites/default/files/anthem-ra-cap.pdf [https://perma.cc/T3U5-2GWK] (obligating Anthem to pay $16 million to the Department of Health and Human Services and to implement corrective measures subject to audit for two years); *see also Resolution Agreements*, DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html [https://perma.cc/G27Z-J8UL] (listing HIPAA violations and resolution agreements).

Many claims are brought against breached entities by other businesses.[60] Banks and other financial institutions often assume substantial costs by resolving fraudulent charges, reimbursing victims, and bringing claims for indemnification through the complex network of contracts that govern the payment card industry.[61] Data is frequently transferred between organizations and data processing vendors with the liabilities often governed by contract.[62] Breached organizations that hold insurance policies must frequently litigate whether the breached entity fulfilled whatever obligations they assumed in the agreement or whether they were at fault in some way that would preclude a payout.[63]

B. Consumer Data Breach Litigation: A Wild Horse Like No Other

Common law theories and traditional enforcement schemes that adequately served the physical world are often an imperfect fit when applied to cyber issues.[64] One of the most prescient examples of this is the evolution of inter-

---

[60] *See* Maleske, *supra* note 2 (discussing data breach litigation brought by businesses and payment card industry actors); s*ee also, e.g.*, Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421, 423 (5th Cir. 2013) (finding that the issuer banks were sufficiently foreseeable victims of Heartland's negligence to allow a negligence claim in the absence of a contractual remedy).

[61] *See* Dawn Causey et al., *Banks Turn to the Courts for Data Breach Claims*, ABA BANKING J. (Sept. 13, 2018), https://bankingjournal.aba.com/2018/09/banks-turn-to-the-courts-for-data-breach-claims/ [https://perma.cc/FP4U-P67F] (noting that banks often incur the costs of fraudulent charges and identity theft resulting from third-party breaches). Card-issuing banks are required by federal law to indemnify card-holders for certain fraudulent charges. *See* 15 U.S.C. § 1643(a) (2018) (limiting credit-card-holder liability for unauthorized use); Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 807 (7th Cir. 2018) (discussing that financial institutions must seek indemnification for their fees through the web of contracts connecting the many intermediaries involved in payment card processing); 12 C.F.R. § 205.6 (2020) (limiting debit-card-holder liability for unauthorized use); *see also* Schnuck Mkts., Inc. v. First Data Merch. Servs. Corp., 852 F.3d 732, 735–39 (8th Cir. 2017) (exploring the intricacies of this contractual relationship following a data breach).

[62] *See, e.g.*, Silverpop Sys., Inc. v. Leading Mkt. Techs., Inc., 641 Fed. App'x 849, 851 (11th Cir. 2016) (discussing the data breach that occurred when a vendor's system was compromised and granted access to the principal's systems); *see also infra* note 121 and accompanying text (discussing state statutes that require covered businesses to contractually obligate third parties to security standards).

[63] *See* Kesan & Hayes, *supra* note 9, at 229–36 (discussing the trends of data breach coverage and how costs are increasing); *see, e.g.*, RSVT Holdings, LLC v. Main St. Am. Assurance Co., 136 A.D.3d 1196, 1198 (N.Y. App. Div. 2016) (holding that data breach liability costs were excluded from the general liability policy). *But see* Travelers Indem. Co. v. Portal Healthcare Sols., L.L.C., 644 F. App'x 245, 248 (4th Cir. 2016) (finding that a general liability policy covered data breach costs and litigation). It is becoming rarer for both general liability policies and specialized cyber insurance policies to cover data breaches as claims become more prevalent. *See generally* Kesan & Hayes, *supra* note 9, at 248–63 (studying cyber-insurance policy litigation data and finding that such cases are increasing and are more often won by insurers). Additionally, these policies are often capped and these policy limits have been decreasing over the previous years. *See* COUNCIL OF INS. AGENTS & BROKERS, *supra* note 49, at 4–5.

[64] *See generally* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (arguing that novel situations in cyberlaw can be accounted for by properly understanding how traditional doctrines apply); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) (arguing in favor of traditional enforcement schemes despite new difficulties posed by connec-

mediary liability doctrines to address the issue of piracy and intellectual property infringement on the internet.[65] The traditional doctrines that previously accounted for the needs of the copyright holders struggled with the scale of activity the internet enables, as well as whether some solutions were even technologically feasible.[66] This led to the passage of the Digital Millennium Copyright Act that created a compliance scheme that obviated some of these difficulties by clarifying liabilities and duties in this new dynamic.[67]

Much of the common law evolved to force those who posed the risk to another to internalize the cost of that risk.[68] In the data breach context, the boundaries of many of these common law principles are tested by the novel dynamic of risks posed by the data economy.[69] Pre-trial litigation essentially comprises the entirety of the battle: no data breach case has gone to trial, and merely surviving a motion to dismiss, one of the lowest thresholds for the viability of a claim, is a huge victory for plaintiffs.[70] In many cases, the outcome

---

tivity); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (exploring the differences between the physical world and the virtual world and how key differences frustrate some attempts to apply common law doctrines); David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365 (2002) (making the exceptionalist argument cautioning against traditional regulation of the poorly understood internet).

[65] *See* Lemley & Reese, *supra* note 5, at 1354–56 (detailing the trend that emerged in internet infringement cases of suing the facilitators of infringing conduct rather than the actual perpetrators for several strategic reasons). *See generally* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984) (determining the standard for intermediary liability that prevented producers of VHS cassette tapes from being held liable for facilitating the infringing actions of others because they were capable of substantial non-infringing uses); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) (dismissing claims of infringement against online service provider on contributory and vicarious liability theories).

[66] *See* Lemley & Reese, *supra* note 5, at 1374–77 (explaining how the connectivity of the internet shifted the dynamics of copyright infringement and frustrated traditional enforcement schemes).

[67] *See id.* at 1346–49 (recounting the development of secondary liability in digital copyright infringement cases, the passage of the Digital Millennium Copyright Act to clarify this liability, and the subsequent limitations to its provisions by various court rulings); *see also* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.).

[68] *See* Kneisner & Leeth, *supra* note 5, at 573–74 (explaining how tort theories evolved to account for market failures that fail to efficiently or equitably allocate the costs of unsafe products); Alan Schwartz, *Proposals for Products Liability Reform: A Theoretical Synthesis*, 97 YALE L.J. 353, 384–88 (1988) (exploring products liability and how industry developments have both frustrated and shaped developments in this field).

[69] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 6–9 (noting cybersecurity issues that have existed since the 1970s); SCHNEIER, *supra* note 8, at 31–33 (discussing the systemic difficulties of cybersecurity); E-COMMERCE AND INTERNET LAW, *supra* note 4, § 2.02[1] (discussing how the common law has evolved to meet the challenges of cyberspace); *see also* Lemley & Reese, *supra* note 5, at 1379–81 (explaining how intermediary liability theories in online copyright infringement cases do not adequately deter the behavior of the actual infringing actor).

[70] *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. at 317–18 (assessing the fairness of the proposed settlement terms in reference to the risk and expense of further litigation in an area lacking clear precedent); *see also* Brief of the Chamber of Commerce of the United States as Amicus Curiae in Support of Appellees, *supra* note 5, at 23–24 (lamenting that large class action lawsuits like

of early proceedings influences whether parties will settle and what bargaining power each side has in such negotiations.[71]

Data breach litigation shares key features with intellectual property infringement litigation by seeking to hold intermediaries liable for the acts of third-parties under the theory that they had a duty to prevent such acts.[72] Difficulties in assessing technological capabilities and industry standards greatly complicate the development of workable standards of care.[73] A similar lack of precedent encourages plaintiffs to creatively assert any and every cause of action they think may survive a motion to dismiss due to the difficulty of predicting which ones may succeed.[74]

---

those that follow breaches are rarely decided on the legal merits but rather result in *in terrorem* settlements).

[71] *See* Allison Grande, *Data Breach Suits Find Easier Path with DC Circ. Ruling*, LAW360 (Aug. 3, 2017), https://www.law360.com/articles/951179/data-breach-suits-find-easier-path-with-dc-circ-ruling [https://perma.cc/5KQG-CR64] (discussing the importance of standing and class certification to data breach plaintiffs and how venue selection is affected by the circuit split on standing); *see, e.g.*, *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2019 WL 387322, at *5–8 (N.D. Cal. Jan. 30, 2019) (detailing the thorough procedural history of the consolidated multi-district litigation as it pertained to class size and certification leading up to the proposed settlement); Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 4–6 (providing a timeline of the class certification process and concurrent mediation sessions that resulted in a proposed settlement).

[72] *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 392–94 (6th Cir. 2016) (Batchelder, J., dissenting) (dissenting due to the intervening third party criminal act breaking chain of causation); *see also* Lemley & Reese, *supra* note 5, at 1346–49 (explaining the emergence of suing the facilitators of online infringement activity rather than the actual perpetrators).

[73] *See, e.g.*, *LabMD, Inc.*, 894 F.3d at 1236–37 (finding the FTC order too vague to enforce due to a complete lack of meaningful standards). The court imagined a scenario where such standards were litigated and found it to be unworkable given the lack of industry consensus on what security features are reasonable. *Id.*; *see* Brief of the National Technology Security Coalition as Amicus Curiae in Support of Petitioner and Vacatur at 13–17, 19–21, *LabMD, Inc.*, 894 F.3d 1221 (No. 9357) (advocating that the proposed FTC standards were based on a hindsight analysis of the attack and that the uncertain compliance standard laid out would present compliance issues and have adverse consequences on the industry).

[74] *See, e.g.*, Stollenwerk v. Tri-West Health Care All., 254 F. App'x 664, 665 (9th Cir. 2007) (affirming the grant of summary judgment against a claim that attempted to analogize data breaches to and extend precedent from cases involving exposure to toxic substances with unclear future risks that are remedied with pre-harm medical monitoring); *see also* Price V. Fishback & Shawn E. Kantor, *The Adoption of Workers' Compensation in the United States, 1900–1930*, 41 J.L. & ECON. 305, 316 (1998) (discussing the increase in litigation actions due to the uncertain legal standards surrounding workplace accidents prior to the implementation of the Workers' Compensation system). *See generally* Consolidated Master Complaint at 70–108, Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333 (W.D.N.Y. 2018) (No. 6:15-cv-06569) (alleging eight counts under common law theories including negligence, negligence per se, breach of contract, and unjust enrichment, as well as statutory causes of action under more than ten state statutes).

1. Standing

One of the first major battlegrounds that data breach plaintiffs face is standing to sue under Article III of the United States Constitution, which determines whether a federal court will even hear the case.[75] Standing requires (1) an injury-in-fact, that is (2) fairly attributable to the conduct of the defendant, and (3) that the harm is redressable through litigation.[76] The ruling in *Clapper v. Amnesty International USA* has had significant implications on how courts regard unclear or difficult to calculate harms by raising the threshold of how likely these future harms are to materialize for standing to be found.[77] The Supreme Court stated that speculative future harms must be "certainly impending" or pose a "substantial risk" of occurring in order for plaintiffs to satisfy the injury-in-fact prong.[78]

---

[75] *See* U.S. CONST. art. III, § 2 (creating the standing requirement implicitly by levying the judicial power to hear true cases in controversy to the courts); John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 204 (2013) (discussing how standing provides a challenge for data breach plaintiffs). Generally, standing is a federal constitutional issue and does not bar state courts from hearing common law or state statutory causes of action—these are likely to be resolved by state constitutions. *See generally* Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE, AGRIC. & NAT. RESOURCES L. 349 (2016) (examining the development of state constitutional standing doctrines). Article III standing is of particular importance to data breach plaintiffs because the putative class is likely to be spread across all fifty states, so the federal court system is more advantageous and better able to accommodate a national class. *See* E-COMMERCE AND INTERNET LAW, *supra* note 4, § 26.15 (discussing data privacy class action litigation and the benefits of federal court jurisdiction in handling large distributed classes).

[76] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408–09 (2013) (detailing the requirements of Article III standing). While courts readily recognize the redressability of identity theft as it pertains to standing, credit monitoring and credit freezes remedy only some of the fraudulent activity and cannot protect against several other types of identity theft. *See Remijas*, 794 F.3d at 696–97 (finding the plaintiffs' harms redressable through credit monitoring and reimbursement of costs); PRIVACY RIGHTS CLEARINGHOUSE, IDENTITY THEFT MONITORING SERVICES 1–2 (rev. 2019) (stating that credit monitoring primarily protects against "new account fraud"). Credit monitoring will alert consumers to when new accounts are opened in their name, but does not actually prevent it, nor does it prevent existing account fraud or tax fraud. PRIVACY RIGHTS CLEARINGHOUSE, *supra*, at 1–2. Credit freezes prevent new accounts from being opened and new federal legislation has made such freezes free. *Id.*; *see also* 15 U.S.C. § 1681c-1(a)(i) (2018) (requiring consumer reporting agencies to provide consumers with free credit freezes upon request).

[77] *See Clapper*, 568 U.S. at 408–09 (clarifying the Article III standing standard to be used for speculative future harms); Attias v. CareFirst, Inc., 865 F.3d 620, 626–30 (D.C. Cir. 2017) (explaining the importance of *Clapper* in the data breach context). *Clapper* involved a challenge to the Foreign Intelligence Surveillance Act and ultimately clarified that the objectively reasonable likelihood standard used by the Second Circuit did not suffice for standing. *See* 568 U.S. at 404–09.

[78] *Clapper*, 568 U.S. at 408–09. At least one scholar has made the case that *Clapper* does not (or should not) present a challenge to data breach litigants who are asserting only increased risk of future injury. *See* Nicholas Green, Note, *Standing in the Future: The Case for a Substantial Risk Theory of "Injury in Fact" in Consumer Data Breach Class Actions*, 58 B.C. L. REV. 287, 288–89, 316 (2017) (discussing the case law support for a lower substantial risk threshold in a set of environmental and public harm cases that are in some ways analogous to data breach litigation).

Courts disagree over how to apply this standard and whether to extend standing to putative future victims.[79] Plaintiffs who have already had their data misused and can prove damages generally have no issue alleging an injury-in-fact, but the "certainly impending" standard is problematic for victims that only allege a heightened risk of future identity theft.[80] In 2010, the Ninth Circuit Court of Appeals held in *Krottner v. Starbucks Corp.* that the compromised consumers had alleged a credible threat of real and imminent harm because unencrypted PII had been maliciously stolen.[81] In 2015, the Seventh Circuit Court of Appeals held in *Remijas v. Neiman Marcus Group* that a malicious hacking attack essentially implies that damage will be forthcoming.[82] The D.C. Circuit Court of Appeals similarly concluded in 2017 in *Attias v. CareFirst, Inc.* that the criminal aspect of a malicious data breach considerably lessens the speculative nature of future injuries.[83]

---

[79] *Compare In re* Zappos.com, Inc., 888 F.3d 1020, 1025 (9th Cir. 2018) (finding that increased risk of identity theft suffices for Article III standing six years after the cases were filed and consolidated), *and Attias*, 865 F.3d at 628 (finding that increased future risk of identity theft was sufficient for standing), *and Remijas*, 794 F.3d at 693 (same), *with* Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017) (finding increased risk of future identity theft insufficient for standing), *and In re* SuperValu, Inc., 870 F.3d 763, 774 (8th Cir. 2017) (same), *with* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (same), *and* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (same). A District of Maryland court recently acknowledged in a consolidated set of bellwether claims testing the viability of various causes of action in regard to the Marriott breach that a "growing number of courts" have begun to recognize the loss of data as sufficient to establish injury-in-fact. *See In re*: Marriott Int'l, Inc., Customer Data Sec. Breach Litig., MDL No. 19-md-2879, 2020 WL 869241, at *9 (D. Md. Feb. 21, 2020) (finding sufficient loss of value resulting from the theft of personal information to establish injury-in-fact).

[80] *See, e.g.*, *In re SuperValu, Inc.*, 870 F.3d at 774 (affirming dismissal of claims by plaintiffs alleging injury solely on the basis of increased future risk but finding standing for plaintiff who alleged actual injury).

[81] *See* 628 F.3d 1139, 1143 (9th Cir. 2010) (finding standing for plaintiffs that had not yet suffered harm, but faced a sufficient likelihood of future harm); *see also In re Zappos.com, Inc.*, 888 F.3d at 1025 (finding that *Krottner* still controls data breach litigation in the Ninth Circuit following *Clapper* and *Spokeo* and that increased future risk from stolen credit card information suffices as a concrete injury). *Krottner* involved the physical theft of a laptop from Starbucks's property, containing unencrypted employee data including the SSNs of approximately 97,000 employees. 628 F.3d at 1140.

[82] *See* 794 F.3d at 693 (finding the harm less speculative when the data breach was perpetrated by criminal actors). *Remijas* involved a malware-based attack that allowed hackers to exfiltrate credit card data. *Id.* at 689–90. The Sixth Circuit also followed this reasoning. *See Galaria*, 663 F. App'x at 387–89 ("There is no need for speculation where . . . data has already been stolen and is now in the hands of ill-intentioned criminals.").

[83] *See* 865 F.3d at 628 (finding standing for plaintiffs who had yet to suffer harm). *Attias* involved the infiltration of a network of computers by hackers who were then able to access the allegedly improperly encrypted PII. *Id.* at 623. The District of Maryland echoed this rationale in their recent ruling in the multi-district litigation following the Marriott breach, stating that the strong evidence of malicious conduct elevated the "actual and threatened harm out of the realm of speculation and into the realm of sufficiently imminent and particularized . . . ." *See In re*: *Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 2020 WL 869241, at *6 (comparing and distinguishing several cases with varying levels of evidence of misuse and finding that the facts of the Marriott breach supported a finding of standing).

While those circuits have found that unauthorized access implies misuse, others have required a stronger showing that the data was or will be misused to survive the pleading stage.[84] The Third Circuit Court of Appeals found the risk of injury to be too speculative in 2011 in *Reilly v. Ceridian*, where forensic data showed that hackers had potentially gained access to data, but not that they definitively did so.[85] Similar defects proved fatal in 2017 in the Fourth Circuit Court of Appeals in *Beck v. McDonald*, in the Second Circuit Court of Appeals in *Whalen v. Michaels Stores, Inc*, and in the Eighth Circuit Court of Appeals in *In re Supervalu, Inc*.[86]

Standing is especially important for data breach litigants because it can determine the size of the class of plaintiffs, and with it, their bargaining power.[87] Generally, only a small subset of compromised data subjects can prove unreimbursed fraudulent charges, so the determination on whether plaintiffs who have yet to suffer harm may be included is highly determinative of the class size and whether the suit will be pursued beyond the class certification stage.[88] The 2016 Supreme Court ruling in *Spokeo, Inc., v. Robins*, that procedural violations of the Fair Credit Reporting Act do not grant consumers standing without further injury that is both "concrete and particularized," has had further implications for data breach plaintiffs.[89] This has limited potential class siz-

---

[84] *See, e.g.*, *In re SuperValu, Inc.*, 870 F.3d at 774 (finding increased risk of future identity theft insufficient for standing); *Beck*, 848 F.3d at 266–67 (same); *Whalen*, 689 F. App'x at 90–91 (same); *Reilly*, 664 F.3d at 42 (same).

[85] *See* 664 F.3d at 42 (finding increased risk of future identity theft insufficient for standing where it could not be shown that the hacker read or accessed the data or that they had malicious intent).

[86] *See In re SuperValu, Inc.*, 870 F.3d at 774 (affirming dismissal of claims by alleging injury solely on the basis of increased risk of identity theft); *Beck*, 848 F.3d at 266–67 (affirming the dismissal and summary judgment of two joined cases involving physical data loss where it could not be definitively shown to have been stolen and not misplaced); *Whalen*, 689 F. App'x at 90–91 (affirming dismissal for lack of standing because plaintiff had already incurred and been reimbursed for fraudulent charges and had canceled the compromised credit card). *Beck* involved two cases, one the physical theft of an unencrypted laptop and the other an instance of several boxes of records headed for storage being misplaced. 848 F.3d at 267–68.

[87] *See, e.g.*, *Remijas*, 794 F.3d at 695 (analyzing injury-in-fact when fraudulent charges had already been reimbursed and stating that these harms would not be redressable, but that these plaintiffs would still face the same risks of future identity theft that entitle them to mitigation expenses); Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016) (dismissing the claims of plaintiffs who had already been reimbursed for fraudulent charges as this negated any actual harm). Far beyond the scope of this Note are the issues of class certification, but class size is of great importance to data breach litigants. *See* 140 AM. JUR. TRIALS 327, § 8 (2020) (discussing why class action suits tend to be beneficial in the data breach context). Due to the fairly low individual harms most data breaches pose to a large group of data subjects, the costs of litigating such an issue would greatly outweigh the benefits to individual plaintiffs from doing so. *See id.* § 16; *see also* Black, *supra* note 75, at 204 (discussing "[d]ata breach class certification hurdles").

[88] *See supra* note 87 and accompanying text.

[89] *See* 136 S. Ct. 1540, 1544 (2016) (stating that procedural violations of the Fair Credit Reporting Act (FCRA) do not suffice for Article III standing without some further provable injury as a result of the violation); *see also* 15 U.S.C. § 1681 (2018) (creating jurisdiction for federal courts to hear

es in statutory causes of action because even if the breach has violated the statute, plaintiffs must plead some further concrete injury to be granted standing.[90]

Plaintiffs' pleadings are tested early in regards to causation as well, with courts requiring some level of proof that the breach caused the fraudulent charges or increased risk of harm prior to discovery.[91] The Seventh Circuit Court of Appeals found in *Remijas* that plaintiffs had standing to sue despite several data breaches occurring around the same time that could have exposed that data.[92] The court stated that the breach notifications received by the class of plaintiffs rendered their claims sufficiently unspeculative to proceed and that any claims that the harm was caused by other breaches would be borne out at a later stage of the litigation.[93]

2. Torts and Contracts

Many data breach litigants bring causes of action alleging negligence or privacy torts against organizations that fail to protect their data.[94] These claims face difficulty on a number of fronts concerning the duty of care owed to consumers and how to qualitatively evaluate what that duty of care requires.[95]

---

private causes of action on the basis of violations of the FCRA). The FCRA created both public regulatory duties for consumer reporting agencies as well as giving wronged consumers a private cause of action under the statute. 15 U.S.C. § 1681. The *Spokeo* ruling has implications for any statutory cause of action as standing will no longer be granted for bare procedural violations but requires a further showing of injury. *See* 136 S. Ct. at 1544.

[90] *See, e.g.*, Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 17 (D.D.C. 2019) (dismissing negligence *per se* claim because plaintiffs did not adequately allege actual harm). *Spokeo* has had implications for potential negligence *per se* claims that allege violation of a statute that establishes a duty, because plaintiffs must still plead actual harm. *See id.*; *see also In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 631, 639–40 (3d Cir. 2017) (determining that plaintiffs pleaded a sufficiently concrete and particularized claim under the FCRA).

[91] *See, e.g.*, *Remijas*, 794 F.3d at 696 (considering the causation prong of Article III standing). At least one judge, however, has opined that causation cannot be established in hacking breaches because the third-party criminal act breaks the chain of causation. *See Galaria*, 663 F. App'x 392–94 (6th Cir. 2016) (Batchelder, J., dissenting).

[92] *See* 794 F.3d at 696 (considering the causation prong of Article III standing in a case involving a data breach that occurred close in time to another major breach and finding that plaintiffs had nevertheless made sufficient allegations for standing purposes).

[93] *Id.*

[94] *See, e.g.*, Rollins v. City of Albert Lea, 79 F. Supp. 3d 946, 960–62 (D. Minn. 2014) (dismissing a privacy tort claim of intrusion upon seclusion); *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1172–76 (asserting a claim of negligence as a breach of duty to reasonably safeguard the data); Rowe v. Unicare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391, at *9 (N.D. Ill. Jan. 5, 2010) (denying a motion to dismiss for plaintiffs' invasion of privacy claims after personal health information had been exposed online due to improper security). *See generally* Jordan Elias, *Course Correction—Data Breach as Invasion of Privacy*, 69 BAYLOR L. REV. 574 (discussing the use of privacy torts in data breach actions).

[95] *See LabMD, Inc.*, 894 F.3d at 1236–37 (explaining the difficulty of applying a reasonable security standard across many types of organizations). Should a data breach case ever go to trial, proving

They also depend heavily on state law precedents and can be further complicated by the multijurisdictional nature of data breach suits.[96]

Negligence claims are plead as a breach of duty to reasonably safeguard the data or the negligent misrepresentation that the data would be secure.[97] The existence of this duty can be unclear in the absence of a contract and some courts even hold that the presence of a contract precludes additional recovery in tort.[98] Plaintiffs who can establish a duty of care would then face the challenge of framing the defendants' behavior as a breach of that duty, requiring a highly technical analysis of an organization's preparedness and the facts of the breach.[99]

Negligence claims are sometimes barred by the economic loss doctrine of torts that limits recovery for economic damages when unaccompanied by property damage or physical injury.[100] The economic loss doctrine traditionally served as a limitation to liability as a matter of public policy; holding organizations liable for the unforeseeable economic harms created indirectly by their actions could potentially create excessive litigation and an unworkable economic system.[101] In regards to data breach litigation, some states adhere to this policy strictly, while others apply it subject to exceptions based on whether an independent duty, special relationship, or foreseeability of harm exists between the parties.[102]

---

reasonable security measures were taken would be a highly contentious issue barring obvious gross negligence. *See id.*

[96] *See, e.g.*, *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1172–76 (discussing the common law precedents of eleven different states in an attempt to determine which states' residents will be included in the plaintiff class); *In re*: Target Corp. Customer Data Sec. Breach Litig., 11 F. Supp. 3d 1338, 1339 (J.P.M.L. 2014) (transferring those thirty-three actions pending in eighteen federal districts to the District of Minnesota, but also noting an additional seventy one potentially joinable actions pending in thirty five districts).

[97] *See, e.g.*, *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1170; *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1311 (D. Minn. 2014) (denying a motion to dismiss for negligent misrepresentation by omission claim).

[98] *See, e.g.*, *Attias*, 365 F. Supp. 3d at 17–26 (D.D.C. 2019) (finding that the presence of a contractual arrangement precluded tort recovery and dismissing several tort theories of recovery, but allowing unjust enrichment claims to go forward).

[99] *See LabMD, Inc.*, 894 F.3d at 1236–37 (musing on the difficulty of potentially litigating such a technical analysis); 140 AM. JUR. TRIALS 327, *supra* note 88, § 18 (explaining the difficulties posed by the technical aspects of data breach cases and that expert witnesses and discovery are often needed to assess the merits of a potential breach of a duty to safeguard data).

[100] *See, e.g.*, *Longenecker-Wells*, 2015 WL 5576753, at *5 (finding a negligence claim precluded by the economic loss doctrine); *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1171–76 (discussing the economic loss rule under the common law of more than ten states and the District of Columbia).

[101] *See, e.g.*, *Longenecker-Wells*, 2015 WL 5576753, at *15–17 (citing the policy argument in favor of limiting tort liability that would otherwise put undue strain on industry and the economy as a reason for dismissal of negligence claim).

[102] *See Attias*, 2019 WL 367984, at *11 (finding no independent duty that would bar the economic loss rule from precluding the tort claims); *Target*, 66 F. Supp. 3d at 1171–76 (discussing the various

The transactional nature of many data subject-data controller relationships means that there are often several putative contract claims that can be alleged.[103] The ubiquitous online contracts generally include privacy policies that guarantee protective efforts against unauthorized disclosures and plaintiffs can assert that this guarantee was deceptive or simply breached.[104] In some states, statutes require companies to provide their privacy policy to any prospective data subject.[105] As a result, many contract theories of recovery are employed by data breach litigants including breach of contract, unjust enrichment, and other common law contract theories.[106] Additionally, instances arise where no formal contract is signed, but plaintiffs allege a breach of implied contract, often arising from a payment card transaction.[107]

---

formulations and exceptions of state economic loss rules barring negligence claims); Caroline M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 357 (discussing the differences in state economic loss doctrines and exceptions).

[103] *See, e.g.*, Amended Complaint for Gross Negligence; Bailment; Breach of Implied Contract; Breach of Express Contract et al. at 17–20, *In re*: YAHOO! Inc. Customer Data Sec. Breach Litig., 2019 WL 387322 (N.D. Cal. 2019) (No. 16-MD-02752-LHK) (outlining the claims of breach of express contract, breach of bailment, and violation of state consumer protection act). *See generally* Consolidated Master Complaint, *supra* note 74, at 77–88 (alleging breach of contract, breach of implied covenant of good faith and fair dealing, third-party beneficiary claim for breach of contract under federal law, negligent misrepresentation of the security practices purportedly guaranteed by their privacy policy, and unjust enrichment).

[104] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240–41 (3d Cir. 2015) (describing the FTC's allegations that Wyndham's guarantees of security were deceptive). Simply giving users an opportunity to read the contract is usually sufficient to put them on inquiry notice that they are agreeing to terms of use; many standard internet browsewrap contracts instruct consumers that proceeding with the use of the service constitutes agreement without requiring them to actually click into or read the terms. *See, e.g.*, Fteja v. Facebook, Inc., 841 F. Supp. 2d 829, 834–41 (S.D.N.Y. 2012) (discussing browsewrap and clickwrap contracts and the inquiry notice standard). Another standard type of internet contract, the clickwrap contract, does require users to click into and sometimes scroll through the terms of use before they are allowed to accept them. *See id.*

[105] *See, e.g.*, CAL. BUS. & PROF. CODE § 22575 (West 2020) (requiring organizations that collect PII to create and provide consumers with a privacy policy); TEX. BUS. & COM. CODE ANN. § 501.052 (West 2019) (requiring the same for organizations that collect SSNs).

[106] *See, e.g.*, *Attias*, 2019 WL 367984 at *5, *7–8 (analyzing plaintiffs' claims of breach of contract and loss of benefit of the bargain theories); *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1176–78 (discussing plaintiffs' claims of breach of implied contract, breach of contract, and unjust enrichment); Consolidated Master Complaint, *supra* note 74, at 77–88 (alleging breach of contract, breach of implied covenant of good faith and fair dealing, third-party beneficiary claim for breach of contract under federal law, negligent misrepresentation of the security practices purportedly guaranteed by their privacy policy, and unjust enrichment).

[107] *See e.g.*, *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1176–78 (discussing plaintiffs' claims of breach of implied contract arising from their use of a credit card that putatively guarantees the secure use of that payment card as part of the transaction); Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011) (alleging successfully that an implied contract was created with the merchant by the credit card transaction); Lovell v. P.F. Chang's China Bistro, Inc., No. C14-1152-RSL, 2015 WL 4940371 (W.D. Wash. Mar. 27, 2015) (finding that a unilateral expectation of payment card security did not create an implied contract).

3. Regulatory Enforcement, State and Federal Statutes, and the General Data Protection Regulation (GDPR) of the European Union

Despite the absence of an overarching cybersecurity statute, or perhaps as a result of it, both data subjects and government entities often attempt to bring actions under various federal and state statutes.[108] Federal statutes such as the Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act, and Graham-Leach-Bliley Act have created information security duties on certain industries or types of data.[109] The Fair Credit Reporting Act established a duty for consumer reporting agencies to avoid unauthorized disclosures of consumer data and created a private cause of action that data subjects have used to assert violations directly.[110] Publicly traded companies are governed by the Securities Exchange Act that creates both regulatory and shareholder causes of action in the wake of data breaches.[111]

The Federal Trade Commission (FTC) has emerged as the main federal regulator of data breaches through its general consumer protection powers as well as by narrow grants of sector-specific statutory authority.[112] Section Five

---

[108] *See* Boyne, *supra* note 3, at 299–304, 332–33 (detailing the federal legislation and regulatory environment that has emerged due to the lack of a comprehensive framework on data security). *See generally In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1161–66 (discussing the claims brought under the consumer protection statutes of forty-nine states and the District of Columbia in the consolidated multijurisdictional litigation); Consolidated Master Complaint, *supra* note 74, at 89–108 (alleging causes of action under state consumer protection laws, state data breach statutes, and state insurance statutes).

[109] *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.) (creating data security standards for financial data); Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6505 (2018) (creating requirements for the collection of personal information from children under the age of thirteen); Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15 U.S.C. and 18 U.S.C.) (creating data security and risk disclosure obligations for publicly traded companies); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections in 18 U.S.C., 29 U.S.C., and 42 U.S.C) (creating data security standards for health information).

[110] *See* 15 U.S.C. § 1681 (creating a private cause of action for liability under the FCRA); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d at 631 (detailing the alleged violation of the FCRA asserted as a cause of action by the plaintiffs).

[111] *See, e.g.*, Second Amended Class Action Complaint for Violations of the Federal Securities Laws, *supra* note 56, at 2–8 (alleging that a class of shareholders of Yahoo stock were harmed by failures to safeguard data and to disclose the breach); *see also* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, *supra* note 50, at *7–13 (providing guidance on disclosure obligations for material cybersecurity risks and incidents); DIV. OF CORP. FIN., SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2: CYBERSECURITY (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [https://perma.cc/W3TP-Y25C] (creating cybersecurity risk disclosure obligations and the basis for shareholders to file derivative suits in the context of data breaches for failure to disclose cybersecurity risks or failure to take adequate measure to reduce this risk).

[112] *See* E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.06 (describing a history of FTC enforcement actions for cybersecurity failures); Boyne, *supra* note 3, at 300–04 (detailing the FTC's

of the FTC Act grants the FTC the power to bring general consumer protection enforcement actions against deceptive or unfair trade practices; although it was never expressly authorized to use this power in data security actions, it was allowed to do so in 2015 by the Third Circuit Court of Appeals in *FTC v. Wyndham Worldwide Corp.*[113] The Third Circuit found that representations of adequate data security practices to consumers in privacy policies could be characterized as an unfair business practice when such practices were clearly not implemented.[114]

Despite some limits to the precedent set in *Wyndham*, the FTC has issued a series of enforcement actions, data security rules, and consent decrees that resemble post-breach settlements.[115] Businesses are generally willing to enter into these agreements to appease regulators, but the Eleventh Circuit Court of Appeals 2018 ruling in *LabMD, Inc. v. FTC* illustrates the limitations that regulators still face in data breach enforcement actions.[116] The Eleventh Circuit neither firmly held nor disclaimed FTC authority over data breaches, but instead ruled that the FTC's order requiring LabMD to implement reasonable security measures was too vague given the lack of clear industry cybersecurity standards and could not be enforced.[117]

All fifty state legislatures have now passed some form of data breach notification law.[118] Some of these notification laws give consumers private causes

---

regulatory authority under both § 5 of the FTC Act and various statutory grants of authority); *see also* FED. TRADE COMM'N, *supra* note 59, at 4–5 (detailing numerous enforcement actions).

[113] *See* 15 U.S.C. § 45 (codifying the Fair Trade Commission Act grant of power to the FTC to bring enforcement actions for unfair or deceptive business practices); *Wyndham Worldwide Corp.*, 799 F.3d at 244–46 (finding that Wyndham's failure to deliver on the security promised by their privacy policy could have misled consumers and was unfair); *see also LabMD, Inc.*, 894 F.3d at 1237 (vacating the FTC's cease-and-desist order directing LabMD to implement reasonable security due to the vagueness of what this requires). The court in *LabMD* did not reach the issue of FTC enforcement powers but nor did it expressly disclaim them. *See* 894 F.3d at 1231, 1237.

[114] *See Wyndham Worldwide Corp.*, 799 F.3d at 244–46 (finding that the representation of adequate data security practices was clearly unfair considering Wyndham's awareness of repeated breaches of their networks).

[115] *See* FED. TRADE COMM'N, *supra* note 52, at 4–5 (detailing some of the recent enforcement actions); E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.06 (listing several FTC consent decrees related to cybersecurity failings); *see also* 16 C.F.R. § 318.3 (2020) (promulgating the FTC's Health Breach Notification Rule, a data breach notification obligation for entities possessing health information but not covered by HIPAA rules on breach notification).

[116] *See* 894 F.3d at 1237 (demonstrating the limits of FTC enforcement powers due to lack of clear standards and industry consensus on what constitutes reasonable security).

[117] *See id.* at 1231 (assuming arguendo that the FTC can enforce the alleged negligent failure to implement reasonable data security measures as an unfair act or practice); *id.* at 1236–37 (posing a hypothetical scenario of trying to litigate such technology industry standards when considerable room for disagreement tends to exist in that sector); *see also In re* LabMD, Inc., 102 F.T.C. 3099, at *34-35 (2016) (ordering LabMD to comply with several security practices and reporting obligations for a period of twenty years).

[118] *Breach Notification Laws*, *supra* note 56 (listing state breach notification statutes for all fifty states).

of action for failures to notify whereas others vest this power solely to the state's attorney general.[119] States often have their own consumer protection laws that create private causes of action or call for enforcement by regulatory bodies.[120] Eighteen states have set "reasonable" security standards for businesses that own or license the personal information of residents and seven require businesses to contractually extend this requirement to any third-parties who will handle that data.[121]

A small subset of states have enacted unique legislation or regulations that create further cybersecurity obligations.[122] Massachusetts enacted the Written Information Security Procedures regulation in 2010 that created standardized requirements for the creation and maintenance of security plans and risk assessments.[123] The New York Division of Financial Services promulgated a new regulation that creates extra compliance cybersecurity obligations for financial services companies that operate in New York.[124] Vermont passed a law requiring data brokers to register with the state and report certain information.[125] California passed several cybersecurity laws in 2018, including the California Consumer Privacy Act (CCPA), which parallels the General Data Protection Regulation of the European Union (GDPR) in several ways and will create private causes of action as well as public enforcement actions for the misuse of data.[126] California also passed what is being hailed as the first Inter-

---

[119] *See* E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.08[10][A] (exploring the enforcement mechanisms created by the various state statutes); *see, e.g.*, CAL. CIV. CODE § 1798.84 (West 2020) (creating a private cause of action for violations of a breach notification statute); MICH. COMP. LAWS § 445.72(13) (West 2020) (granting enforcement powers to the state Attorney General).

[120] *See In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1172–76 (alleging violations of various state consumer protection statutes); E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.08[10][C] (exploring the regulatory enforcement powers created by state data breach notification statutes, often vested in state attorneys general).

[121] *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (West 2020) (establishing that businesses that own or license personal data of residents have an obligation to implement reasonable security procedures as well as contractually bind any third parties who will handle the data to this standard); COLO. REV. STAT. ANN. § 6-1-713.5(2) (West 2020) (same); MD. CODE ANN., COM. LAW § 14-3503 (West 2020) (same); NEV. REV. STAT. ANN. § 603A.210 (West 2019) (same); TEX. BUS. & COM. CODE ANN. § 521.052(a) (West 2019) (establishing a standard of protection, but not a requirement to extend this duty via contract).

[122] *E.g.*, CAL. CIV. CODE § 1798.91.04 (West 2020); VT. STAT. ANN. tit. 9 §§ 2446–2447 (West 2019); 201 MASS. CODE REGS. 17.00–17.05 (2020); N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2020).

[123] 201 MASS. CODE REGS. 17.00.

[124] N.Y. COMP. CODES R. & REGS. tit. 23, § 500. The regulation applies to entities operating in the financial services industry and creates enhanced cybersecurity and risk assessment obligations, including mandatory penetration testing and vulnerability assessments. *Id.*

[125] VT. STAT. ANN. tit. 9 §§ 2446–2447. The data broker law requires annual registration and disclosure of various pieces of information regarding the collection, usage, and sale of the data. *Id.* § 2446. It also establishes a duty to implement and maintain a comprehensive data security program including employee training and technical safeguards. *Id.* § 2447.

[126] *See* CAL. CIV. CODE § 1798.100 (West 2020) (codifying the California Consumer Privacy Act); Joseph V. Moreno et al., *The Digital Revolution Takes on New Meaning: Among Calls for Heightened*

net-of-Things cybersecurity law in the United States, creating security implementation and design obligations for producers of connected goods.[127] The California laws may come to act as de facto federal legislation due to the size and importance of the California market, which likely will make it cheaper to simply comply with the laws across the board rather than develop state-specific data safety practices.[128]

The GDPR recently enacted by the European Union (EU) is arguably the most comprehensive data protection regime promulgated to date.[129] It applies to any entity that holds data on citizens of the EU and sets out rules for the collection, handling, and processing of that data.[130] Most significantly, it encourages compliance by prescribing extreme penalties—the higher of twenty million euros or four percent of global yearly revenue can be assessed on particularly culpable violators.[131] Additionally, it allows for executives and board members to face liability for data breaches.[132] A recent survey calculated over fifty nine thousand breaches reported under the GDPR between May 2018 and January 2019, and the number of major GDPR fines increased significantly in 2019 over the year prior.[133]

U.S. Data Privacy Measures, California Is King, NAT'L L. REV. (Mar. 1, 2019), https://www.natlawreview.com/article/digital-revolution-takes-new-meaning-among-calls-heightened-us-data-privacy-measures [https://perma.cc/84DM-BUZ2] (discussing the impacts of the California Consumer Privacy Act and comparing several of its provisions to those of the GDPR); *Cybersecurity Legislation 2018*, NAT'L CONF. OF STATE LEGISLATURES, www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx [https://perma.cc/577K-CNJ8] (listing the cybersecurity legislation passed by California in 2018).

[127] *See* CAL. CIV. CODE § 1798.91.04 (creating security design and implementation obligations for connected devices manufactured or sold in California); Timothy Tobin et al., *California Passes First-of-Its-Kind Law Focused on Internet of Things Cybersecurity*, HOGAN LOVELLS (Oct. 17, 2018), https://www.hldataprotection.com/2018/10/articles/consumer-privacy/california-passes-first-of-its-kind-law-focused-on-internet-of-things-cybersecurity/ [https://perma.cc/S86H-78ZJ] (discussing the impact of this legislation).

[128] *See* Travis Brennan et al., *California Sets De Facto National Data Privacy Standard*, CORP. COUNSEL BUS. J. (July 6, 2019), https://ccbjournal.com/articles/california-sets-de-facto-national-data-privacy-standard [https://perma.cc/NDR5-QRGC] (speculating that it would be cost prohibitive for companies that operate on a national scale to develop platforms to cater to the various regulatory requirements of each state, making it cheaper to simply comply with the most restrictive regime).

[129] *See generally* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119/1) (setting standards for the data protection and privacy laws of European Union member states).

[130] *See id.* at art. 2 (providing material scope); *id.* at art. 3 (providing territorial scope).

[131] *See id.* at Ch. VIII, art. 77 (noting remedies, liability and penalties); 6 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW § 51.04 (rev. ed. 2019) (characterizing the severity of GDPR's maximum fines as "draconian" in order to encourage compliance).

[132] *See* Ffion Flockhart et al., *Cyber Risk and Directors' Liabilities: An International Perspective*, NORTON ROSE FULBRIGHT (Dec. 2016), https://www.nortonrosefulbright.com/en-me/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective [https://perma.cc/N7DA-C48F] (detailing director liability in several European countries post-GDPR).

[133] DLA PIPER, GDPR DATA BREACH SURVEY: FEBRUARY 2019, at 3 (2019) (examining some early data breach enforcement actions under the GDPR); *Major GDPR Fine Tracker—An Ongoing*,

II. (I CAN'T GET NO) DATA SECURITY

This Part discusses how the search for a legal remedy for data breach victims has been impeded by the complexity and scope of the issue as well as the potential repercussions of expanding liability in this area.[134] Section A utilizes key systemic features and economic concepts to explore the risks of the data economy and demonstrate the virtual impossibility of securing all consumer data.[135] Section B discusses how these features interplay with the impacts that potential resolutions may have on the economy and innovation.[136]

A. Guaranteed Insecurity: We Like Smart-Fridges More Than Privacy, So We Can't Have Nice Things

Several issues create a likelihood that identity theft will continue to increase and pose challenges to the use of private liability as a regulator of risky behavior.[137] First, the complexity of modern technology virtually assures continued vulnerability and makes litigation functionally impossible and overly cumbersome.[138] Second, both consumers and organizations struggle to analyze the inherent risks of using personal data and fail to account for it, driving greater economic reliance on data.[139]

1. Wile-E Coyote Looks Down: The Realization of Insecure Foundations

The first issue is the inherently vulnerable architecture of the internet and the inability to achieve perfect security.[140] The piecemeal series of additions,

---

Always Up-To-Date List of Enforcement Actions, ALPIN, https://alpin.io/blog/gdpr-fines-list/ [https://perma.cc/EBF2-YVVN] (listing major GDPR enforcement actions).

[134] *See infra* notes 137–200 and accompanying text.

[135] *See infra* notes 137–178 and accompanying text.

[136] *See infra* notes 179–200 and accompanying text.

[137] *See* Shavell, *supra* note 16, at 366–69 (describing the conditions that allow traditional applications of liability to allocate costs efficiently); *see also infra* notes 138–178 and accompanying text.

[138] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 8–9 (explaining the fundamental difficulties in cybersecurity due to the complexity and ad-hoc design of our networks as well as the lack of secure design); *see also infra* notes 139–149 and accompanying text.

[139] *See* SCHNEIER, *supra* note 19, at 235–38 (discussing how the lack of certainty about the risks and the misalignment of priorities between individuals and the general population have resulted in consumers with a strong preference for data-augmented devices and driven data-based innovation); Alessandra Arcuri, *Risk Regulation*, *in* 9 ENCYCLOPEDIA OF LAW AND ECONOMICS 302, 324–25 (2d ed. 2012) (explaining how uncertainty disrupts the cost-benefit analysis); Benjamin E. Hermalin, *Uncertainty and Imperfect Information in Markets*, *in* HANDBOOK OF THE ECONOMICS OF RISK AND UNCERTAINTY, *supra* note 5, at 263, 264–65 (discussing the concepts of imperfect information and information asymmetry and how they influence consumer preferences); *see also infra* notes 150–178 and accompanying text.

[140] *See* SCHNEIER, *supra* note 19, at 141–43 (discussing the attacker-defender dichotomy that makes cybersecurity so difficult); N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 8–9 (listing several reasons why cybersecurity is challenging on a technical level).

upgrades, and patches that the internet and network protocols have undergone have left us with a minefield of vulnerabilities that continue to grow with each new software version.[141] There is no such thing as a bug-free program and the open-access design of many of these programs, a necessary design feature for most internet software that interacts with other programs, virtually assures that exploits will be found by those who dig hard enough.[142] Many internet connected organizations are reliant on an entire inventory of third party devices and software that create a web of vulnerabilities.[143]

At best, a well patched product may prevent known attack vectors, but the "attacker's advantage" in cybersecurity means that security professionals often learn of a vulnerability only after it has been exploited.[144] Human nature can never be fault-free and sterling network architecture and personnel training can be undone by a single honest mistake, such as an employee falling victim to a phishing email and clicking a malicious link.[145]

---

[141] *See* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 54 (2018) (discussing how the forensic investigation of breaches is made difficult by complex networks); N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 8–9 (explaining the fundamental difficulties in cybersecurity due to the complexity and ad-hoc design of our networks as well as the lack of secure design); SCHNEIER, *supra* note 19, at 140–46 (detailing the vulnerabilities created by how complex computer systems are).

[142] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 8 (identifying the open access internet architecture and buggy software as two key reasons why cybersecurity is so challenging); Black, *supra* note 6, at 1–2 (detailing the SARD database of over 170,000 currently known bugs); *see also* SCHNEIER, *supra* note 8, at 129 ("The reason we have the internet is that companies were able to market buggy products .If computers were subject to the same product liability regulations as stepladders, they probably wouldn't be . . . on the market yet.").

[143] *See* SCHNEIER, *supra* note 8, at 20–33 (detailing the myriad design oversights that ensure a system with pervasive vulnerabilities); SCHNEIER, *supra* note 19, at 144–46 (explaining the wealth of endpoints in our interconnected system and the likely presence of hundreds of unknown vulnerabilities in each). Many systems are compromised by the discovery of a single software vulnerability, as every system that runs the software is compromised until patched. SCHNEIER, *supra* note 8, at 31.

[144] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 8–9 (explaining the fundamental advantages that attackers hold over defenders in cybersecurity); SCHNEIER, *supra* note 19, at 141 (detailing the imbalance of power in the attack-defense dynamic and how many vulnerabilities are discovered only after they have caused problems); Matthew Morgan et al., *Network Attacks and the Data They Affect*, *in* DYNAMIC NETWORKS AND CYBER-SECURITY 1, 4–6 (Niall M. Adams & Nicholas A. Heard eds., 2016) (discussing the attacker's advantage as a "cat and mouse" game where defenders must seek to close all vulnerabilities but attackers need only find a single one).

[145] *See* IDENTITY THEFT RES. CTR., *supra* note 28, at 1–2 (discussing the scope of human-targeted attacks such as spearphishing and malware and how they are increasing in prevalence due to their effectiveness); SCHNEIER, *supra* note 8, at 45–46 (discussing the weaknesses in many authentication systems that rely on usernames and passwords and how easy it is for people to fall victim to credential theft); *see also* Steven Shavell, *The Optimal Level of Corporate Liability Given the Limited Ability of Corporations to Penalize Their Employees*, 17 INT'L REV. L. & ECON. 203, 203–04 (1997) (explaining the limited deterrence effect of corporate liability on employee behavior as employees often face no personal liability and how their risk is usually limited to loss of their job). Credential stealing has become very easy, and efforts to phish, social engineer, or otherwise guess logins, passwords, and security phrases are often extremely effective and have led to high profile attacks. SCHNEIER, *supra* note 8, at 45–46.

Attackers are more motivated than ever to discover these profitable exploits, often from the comfort of a home country with no extradition agreement.[146] A large variety of attacks ranging in sophistication have been levied against numerous targets.[147] Mothers'-basement-hackers require little more than a computer and an internet connection to gain access to guides and hacker tools to easily exploit known vulnerabilities.[148] On the other end of the spectrum, sophisticated and well-funded hackers are likely able to use brute force or finesse their way into nearly any system of interest.[149]

2. Incentivized Insecurity: Uncertainty and Imperfect Information, Externalities, and Information Asymmetry

Uncertainty about the risks of compromised privacy results in imperfect information in the data market.[150] Many of the costs of a data breach are borne by intermediaries, creating externalities for both consumers and organizations that muddle the cost-benefit analysis of participation in the data economy.[151]

---

[146] *See Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data, Hearing Before the Subcomm. on Terrorism & Illicit Fin. of the H. Fin. Servs. Comm.*, 115th Cong. 1–5 (2018) (statement of Lillian Ablon, Scientist, RAND Corporation) [hereinafter *Data Thieves Hearing*] (discussing the prevalence of cyberattacks and the different motivations for several types of cyberthieves); *see also* 112 AM. JUR. TRIALS 1, § 1 (2020) (explaining the difficulties of targeting the actual identity thieves and why lawsuits tend to target more reachable intermediaries).

[147] *See Infographic: Identity Thief Toolkit*, IRIS (Sept. 14, 2016), https://www.irisidentityprotection.com/blog/identity-thief-infographic/ [https://perma.cc/6PAF-KFT8] (listing the various cyber threats, such as whaling, smishing, vishing, pharming, and so forth); *Internet Crime Complaint Center*, FED. BUREAU OF INVESTIGATION, https://www.ic3.gov/media/default.aspx [https://perma.cc/5LXB-HDP4] (tracking press releases concerning many different types of active cyber threats).

[148] *See Data Thieves Hearing*, *supra* note 146, at 7–8 (explaining that there are negligible barriers to enter the black market for data given the tutorials, hackers for hire, and hacker tools available to anyone with an internet connection); LILLIAN ABLON & ANDY BOGART, RAND CORP., ZERO DAYS, THOUSANDS OF NIGHTS, at xi (2017) (discussing the market for purchase, sale, and trade of "zero-day vulnerabilities," as yet unknown or addressed vulnerabilities); *see also* CARBON BLACK, THE RANSOMWARE ECONOMY 2 (2017) (finding a 2,500% increase in black market ransomware sales from 2016 to 2017); SCHNEIER, *supra* note 8, at 30 (discussing "script kiddie[s]," a term referring to unskilled hackers who use prepackaged hacker tools and scripts available for purchase or for free online).

[149] *See Data Thieves Hearing*, *supra* note 146, at 3–5 (explaining that state-sponsored actors are often well funded and sophisticated, and their attacks are highly targeted and persistent).

[150] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 8–9 (explaining the risks created by the widespread use of information technology and the lack of incentives for secure design); Arcuri, *supra* note 139, at 324–25 (explaining the effect of uncertain benefits and costs on rational decision-making); Fazzini, *supra* note 11 (reporting the confusion of experts who have yet to identify any traditional uses of the Equifax data and that some suspect that more sophisticated actors may be at work).

[151] *See* WEISS & MILLER, *supra* note 24, at 14–19 (presenting research on the many cost bearers from several large data breaches); *see also* MICHAEL POWER, ORGANIZED UNCERTAINTY 12–21 (2007) (explaining the risk-uncertainty dichotomy and how risk analysis, and therefore behavior, differs across individuals, sectors, classes of actors, and even within organizations); Zhuang et al., *supra* note 9, at 16–18 (modeling a security market and finding considerable inefficiency due to many actors acting in their own interests).

Organizations routinely guarantee some level of data security to their data subjects, but an information asymmetry is created by the inability of consumers to verify or evaluate such guarantees.[152] Consumer willingness to trade personal data for value-adding features creates an incentive for businesses to participate in the data economy, but typically at the expense of privacy and security, which is treated as a poor investment.[153]

Consumers' failure to account for the risks and costs of compromised privacy can largely be attributed to their poor understanding of it.[154] Nearly every app and web service has users agree to "terms of use" that give the companies broad leeway over how user data will be collected, used, and protected.[155] A consumer looking to use a smart device or sign up for a "free" web service is unable to weigh what they are agreeing to due to the abstract nature of personal data risk.[156] Even if they have a rough understanding of the known harms, the future risks of compromised personal data remain poorly understood even to experts.[157]

Externalities also prevent consumers from fully understanding the risks and costs of compromised data.[158] Fraudulent charges, the most concretely identifiable harm, are largely externalized onto financial institutions, so consumers are unlikely to include such costs when consenting to the use of their data as they are unlikely to incur them personally.[159] Similarly, much of the

---

[152] *See* SCHNEIER, *supra* note 8, at 133–34 (explaining how consumers have no practical way of determining whether companies are representing their security procedures accurately); George Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 488–91, 495 (1970) (discussing how information asymmetries encourage dishonest behavior because buyers reward guarantees of quality, but cannot distinguish when these representations are false); *see also* Hermalin, *supra* note 139, at 264–65 (discussing information asymmetries).

[153] *See* Kesan & Hayes, *supra* note 9, at 220–22 (explaining the incentives that prompt businesses to prioritize price over the security of connected products).

[154] SCHNEIER, *supra* note 19, at 235–38 (writing on the unknowable effects of the mass usage of data and how uncertain harms affect our data-use preferences); *see also* Arcuri, *supra* note 139, at 324–25 (explaining how uncertainty regarding the risks of a specific behavior affect the ability of decision makers to make efficient choices).

[155] *See* Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMM., & SOC'Y 128, 129–31 (2020) (discussing the widespread adoption of privacy policies to comply with the "notice and choice" privacy framework of data collection).

[156] *See* SCHNEIER, *supra* note 19, at 235–38 (explaining the nature of data risk to society as a whole and how individuals are prone to ignoring these distributed harms).

[157] *See* SCHNEIER, *supra* note 8, at 50–51 (describing the unknown extent of future identity theft crimes); Fazzini, *supra* note 11 (discussing the confusion of cybercrime experts as to where the Equifax data has gone and what purpose it is being used for).

[158] *See* SCHNEIER, *supra* note 19, at 235–38 (discussing how individuals do not incorporate the distributed group harms of data usage into their decision making); Kesan & Hayes, *supra* note 9, at 220–21 (stating that externalities are pervasive in cybersecurity due to cost spreading and the distribution of harm from these activities over many stakeholders).

[159] *See* 15 U.S.C. § 1643 (2018) (limiting consumer liability unless card issuers provide proper notification channels); 12 C.F.R. § 205.6 (2020) (limiting consumer liability for fraudulent charges

risk of harm is externalized to other data subjects.[160] Consumer data is most valuable to both thieves and businesses when aggregated into massive databases.[161] Individual consumers often receive ample benefit from web services that justify the risk that their data may be compromised, but as more consumers make this exchange, the risk to each data subject grows by virtue of aggregating this data together and making it a riper target.[162]

Many of the costs that data breaches pose to the breached entity are similarly externalized onto consumers and intermediaries.[163] Organizations are incentivized to invest only as much into cybersecurity as is likely to mitigate their own cost of a data breach rather than the entire cost.[164] Employees of organizations are also affected by the unlikelihood that they will be personally held liable and have less incentive to improve behaviors when the company that be the one liable for their errors.[165]

An information asymmetry regarding the level of protection on their data also prevents consumers from understanding the tradeoff between data and

---

only if reported in a timely fashion); HARRELL, VICTIMS OF IDENTITY THEFT 2016, *supra* note 32, at 9 (finding that 88% of victims did not face out of pocket costs, mainly due to reimbursement or fraud protection by financial institutions); *see also* WEISS & MILLER, *supra* note 24, at 19 (listing the various intermediaries who bear costs from a payment card data breach).

[160] *See* SCHNEIER, *supra* note 19, at 235–38 (discussing how the total harm created by data breaches is very large, but tends to be low at an individual level when distributed amongst all stakeholders).

[161] *See* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 18 (2018) (discussing how the massive amount of consumer data held by credit reporting agencies has made them prime targets for attacks).

[162] *See* SCHNEIER, *supra* note 19, at 235–38 (writing on the conflicting group and individual interests that prevent individuals from understanding the cost of the "data trade-off" and mass usage of data); *see also* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 18 (2018) (remarking that data thieves are likely to target large data sets because they tend to be more profitable for the effort).

[163] *See* WEISS & MILLER, *supra* note 24, at 5–7, 14–19 (listing the numerous cost bearers that resulted from several large data breaches); SCHNEIER, *supra* note 8, at 124–28 (lamenting the externalities that misalign the incentives of executives when it comes to investment into cyber risk management); Kesan & Hayes, *supra* note 9, at 220–21 (stating that externalities are pervasive in cybersecurity due to cost spreading).

[164] *See* Zhuang et al., *supra* note 9, at 16–18 (modeling security investment preferences of individuals based on perceived risks to themselves rather than the total harm their activities may cause). When the perceived risk to the individual entity is smaller than the overall risk posed by the activity, the entity is only incentivized to insure their own potential risk exposure. *Id.* Similarly, the presence of various discount factors that reduce the expected return on security investments is likely to prompt less investment. *Id.*

[165] *See* Shavell, *supra* note 16, at 362–63 (explaining that employees often face insufficient incentives to reduce risks because they are both unlikely to bear the full cost of the harm nor face personal liability for it); Shavell, *supra* note 145, at 203–04 (explaining how employee decision makers are less incentivized to prevent harm to the organization because they will not experience the majority of this harm).

privacy.[166] Consumers are likely to receive a generic assurance of reasonable security measures for the storage of their data, but have no feasible way to verify if this is the case.[167] Most consumers either do not read or cannot understand the functional effect of privacy policies and any alternative products are likely to have similar policies, reducing the ability of consumers to shop for greater security.[168] Data brokers buy and sell this data per the agreed upon terms of use, and thus consumers are unlikely to even know who holds their personal data, let alone evaluate the security in place.[169]

While consumers cannot accurately weigh the risks and have no way of knowing how well protected their data will be, they are exceedingly reactive to price.[170] This creates what is known as a Lemons Market: there is no reliable return on investment for security, and as a result, the market is saturated with

---

[166] *See* Hermalin, *supra* note 139, at 264–65 (discussing imperfect information and information asymmetries). Even if this information asymmetry was resolved, however, it is unlikely to help on its own considering the uncertain risks of compromised privacy. *See id.* at 264 (explaining that the value of information is highest when risks are understood).

[167] *See* SCHNEIER, *supra* note 8, at 133–34 (explaining how consumers have no practical way of determining whether companies are representing their security procedures accurately); Akerlof, *supra* note 152, at 488–91, 495 (discussing how information asymmetries create incentives for sellers because to buyers reward guarantees of quality, but cannot distinguish when these representations are false).

[168] *See* Lior J. Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. 69, 92 (2016) (stating that lay consumers do not typically read privacy policies and that when they do they are unable to determine the legal significance of the terms and likely to interpret the clauses in a variety of ways); *see also* SCHNEIER, *supra* note 19, at 61 ("Opting out just isn't a viable choice for most of us . . . . [I]t violates what have become very real norms of contemporary life."). Even if organizations provided their data subjects with a more detailed account of the security procedures in place, consumers would struggle to evaluate the actual protection provided given the complexity of cybersecurity. *See* SCHNEIER, *supra* note 8, at 133–34 (proclaiming that it is difficult even for experts to evaluate guarantees of security).

[169] *See* Bruce Schneier, *It's Not Just Facebook. Thousands of Companies Are Spying on You*, CNN (Mar. 26, 2018), https://www.cnn.com/2018/03/26/opinions/data-company-spying-opinion-schneier/index.html [https://perma.cc/N5KS-RNT4] (explaining that thousands of data broker companies exist and purchase your data legally from those who have collected it). Schneier describes the data broker industry and how companies often sell their data to hundreds of others, so it is generally possible that a given consumer's data is held by thousands of companies, each of them a potential vulnerability. *See id.* Users consent to this sale of their data in most of the terms of use that they agree to. *Id.* Additionally, there are entities, such as credit reporting agencies like Equifax, that collect information on consumers, yet never seek consent nor offer opt-outs. *See* MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 115TH CONG., REP. ON THE EQUIFAX DATA BREACH 13 (2018) (explaining that credit reporting agencies aggregate consumer data without seeking consent or providing an option to opt-out of this collection).

[170] *See* SCHNEIER, *supra* note 8, at 134–35 (describing the information asymmetry that prevents consumers from understanding how secure their data actually is); SCHNEIER, *supra* note 19, at 235–38 (discussing why individuals fail to understand the group risks posed by mass data collection); Akerlof, *supra* note 152, at 488–91, 495 (discussing how the information asymmetry created by a lack of reliable indicators of quality favors lower quality products because these tend to be cheaper and consumers readily understand price).

vulnerable products.[171] Businesses often take the role of consumer and entrust data to third-party software, vendors, or components subject to these same limitations that prioritize low-cost over safety.[172]

The great potential liability that data breaches bring is likely to lead to underinsurance in terms of cybersecurity investment.[173] In some cases, the liability could exceed the value of the organization, and organizations have no incentive to insure beyond their assets.[174] Most organizations simply cannot afford to budget a significant amount towards preparedness because it only provides a return on investment if they experience and detect a breach.[175] Even if reasonable security is implemented, organizations would have to spend considerable resources in litigation to prove this point, further reducing the incentive to invest in cybersecurity.[176] At best, organizations may be able to reduce the probability of a breach by investing in security, but the risk of data breach is pervasive.[177] Cybersecurity preparedness provides diminishing returns after

---

[171] *See* SCHNEIER, *supra* note 8, at 133–35 (describing the lemons market created by cybersecurity information asymmetry that does not reward investments in cybersecurity); *see also* Akerlof, *supra* note 152, at 488–91, 495 (modeling the lemons market that emerges when purchasers are insensitive to quality); Hermalin, *supra* note 139, at 313–17 (discussing exogenous asymmetries of information with informed sellers and uninformed buyers and the resulting lemons model market); Zhuang et al., *supra* note 9, at 16–18 (modeling a dominant strategy of low investment in security when there are high investment costs and discount factors on their return on investment).

[172] *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?*, 13 J. BUS. & TECH. L. 217, 226–27 (2018) (detailing the complexity of the modules, software, and vendor services that many small businesses utilize and the difficulties they face in evaluating or prioritizing security).

[173] *See* Steven Shavell, *The Optimal Structure of Law Enforcement*, 36 J.L. & ECON. 255, 279–80 (1993) (explaining that when organizations do not have the assets to cover potential liability, they are unlikely to be motivated to reduce risks if the risky behavior otherwise generates value).

[174] *See* Shavell, *supra* note 16, at 360–63 (discussing when risky behaviors go underinsured because the cost of the direct harm is externalized or otherwise exceeds the assets of the organization and limits potential liability to that amount); Shavell, *supra* note 173, at 279–80 (stating that when the liability of an organization is capped, such as the amount it would take to go bankrupt, they are unlikely to insure beyond that amount and are thus likely to engage in underinsured risky behaviors).

[175] *See* Shavell, *supra* note 16, at 364 (describing the advantage of underinsuring against "unlikely" events as they only produce a return on investment if the event occurs); *see also* Selznick & LaMacchia, *supra* note 172, at 226–27 (discussing the cybersecurity dilemma faced by many small businesses with limited resources).

[176] *See* Shavell, *supra* note 16, at 368–69 (stating that liability is efficient when some administrative costs can be avoided because suits will not be brought when entities are clearly in compliance with legal standards); *see also* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236–37 (11th Cir. 2018) (discussing the costs and required experts that litigating compliance to reasonable security would require).

[177] *See* MARTIN C. LIBICKI ET AL., RAND CORP., THE DEFENDER'S DILEMMA 99–107 (2015) (recommending that organizations and public policy take a risk management approach that prioritizes the most likely vectors and increases the difficulty level for cybercriminals just enough to make them go elsewhere); STEPHEN B. LIPNER & BUTLER W. LAMPSON, NAT'L INST. OF STANDARDS & TECH., RISK MANAGEMENT AND THE CYBERSECURITY OF THE U.S. GOVERNMENT 1–2 (2016) (explaining how the impossibility of perfect cybersecurity necessitates a risk management based approach that prioritizes cost-effective measures and harm reduction).

the point where the company might realistically defeat litigation or mitigate the costs of potential liability, litigation, and public relations expenditures.[178]

B. Public Policy of Regulating Technology: Which Mountain Do We Move?

Regulating the connected world has long been a contentious topic with many arguing the normative and positive reasons for why, how, and whether or not to do so.[179] This interconnectivity has created novel challenges to the application of previously effective common law remedies and has led to landmark cases and legislation that have been highly influential on innovation.[180] The 1984 Supreme Court ruling in *Sony Corp. of America v. Universal City Studios, Inc.* and the 1995 Northern District Court of California ruling in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.* are often referenced as shaping the development of technology by clarifying the obligation of service providers in the wake of new technology that threatened to disrupt how courts handled intellectual property rights.[181] Similarly, the 2001 Ninth Circuit Court of Appeals ruling in *A&M Records, Inc., v. Napster, Inc.* and the 2005 Supreme Court ruling in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd.*, largely eliminated further development of peer-to-peer sharing networks by extending liability to the operators of these networks as the facilitators of the infringing activity of their users.[182]

---

[178] *See* Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine*, 4 J.L. & CYBER WARFARE 109, 129–33 (2014) (detailing strategies for directors to develop processes that will protect them from potential liability).

[179] *See, e.g.*, Daniel Gervais, *The Regulation of Inchoate Technologies*, 47 HOUS. L. REV. 665, 669–70 (2010) (discussing the effects on innovation of regulating new technologies); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1400–02 (1996) (concluding that the difficulties posed by the connectivity of the internet require that regulation account for special characteristics and avoid overstepping appropriate limits); Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841, 1849–50 (2011) (discussing policy avenues for disruptive technologies).

[180] *See* Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 176–77, 182–85 (2014) (describing the difficulties created by disruptive innovations on regulatory schemes that fit previous frameworks); Johnson & Post, *supra* note 179, at 1370–76 (discussing the futility of traditional notions of governance due to the lack of borders); Lemley & Reese, *supra* note 5, at 1346–49, 1381–86 (detailing the effects on industries of attempts to regulate novel issues posed by technology and the development of the Digital Millennium Copyright Act (DMCA) to address deficiencies in digital copyright infringement enforcement).

[181] *See* Lemley & Reese, *supra* note 5, at 1346–53, 1386–90 (discussing the effect that *Sony* and the DMCA had on the development of innovation around the new boundaries in copyright infringement liability). *See generally* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). The Digital Millennium Copyright Act § 512 largely adopted the standard of intermediary liability in *Netcom*. *See* Lemley & Reese, *supra* note 5, at 1346–53, 1386–90 (describing how the ruling was incorporated into the legislative process behind the DMCA).

[182] *See* Lemley & Reese, *supra* note 5, at 1381–90 (discussing the "loss of the p[eer]2p[eer] dissemination network" in the wake of *Napster* and the then-continuing *Grokster* litigation). *See generally* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (holding that induce-

Solutions that shift liability to the creators of data-integrated products must grapple with the poor understanding of the present costs and harms of data insecurity as well as the future opportunity costs of reducing data-based innovation.[183] The impossibilities of perfect security and the market forces sustaining our use of personal data result in a similar risk posed to each individual data subject from a variety of sources.[184] Courts have struggled to draw reasonable lines in this environment due to these dynamics and the uncertainty accompanying the harm caused by this mystifying new crime.[185]

A strict regime that requires all uses of data to comply with stringent security practices could substantially increase barriers to entry and stymy innovation.[186] A hallmark of the technological revolution is the low barrier to entry—sometimes simply a single computer connected to the internet—to participate in a worldwide economy and create billion-dollar products sans billion-dollar operations.[187] Increasing this barrier will reduce competition by pricing out some of the future Gateses, Musks, and Zuckerbergs to the benefit of the

---

ment of infringing activity creates intermediary liability); A&M Records, Inc., v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (delineating the standards for contributory and vicarious liability in peer-to-peer filesharing networks).

[183] *See* SCHNEIER, *supra* note 8, at 126 (discussing the market effects of forcing data collectors to internalize the costs of harm from this data); Lemley & Reese, *supra* note 5, at 1389 n.171 (describing how it is difficult to project the costs and benefits of "harmful" technologies due to the inherent speculation required and the distribution of societal benefit such innovation brings); *see also* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 28–29 (1970) (stating that attempts to reduce the severity and frequency of accidents through liability must be balanced against the cost of this attempt); Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?*, 50 TEX. INT'L L.J. 305, 315–16 (2015) (discussing how Judge Learned Hand's "risk/utility formula" for negligence applies to cybersecurity preparedness and the practical difficulties it would pose for courts).

[184] *See* SCHNEIER, *supra* note 19, at 140–43 (describing the identical risk posed from each entity that possesses a given set of consumer data); *see also infra* notes 140–178 (discussing the difficulties and market failures that have created an insecure network). Schneier likens the dynamic to a burglar: the burglar doesn't care who they rob and if one house's locks are strong, they will just go next door and rob the neighbor. *See* SCHNEIER, *supra* 19, at 142 (explaining that attackers are opportunistic and choose targets based on vulnerability). Unfortunately, the harm to the data subjects is the same no matter where a given set of data is exfiltrated from. *Id.* Even if most organizations have strong security in place, it only takes one breach for that data to be compromised and made available on the black market to many nefarious entities. *See id.*

[185] *See, e.g.*, Longenecker-Wells v. BenCard Servs., No. 1:15-CV-00422, 2015 WL 5576753, at *16 (M.D. Pa. Sept. 22, 2015) *aff'd*, 658 Fed. App'x 659 (3d Cir. 2016) (describing the difficulty of drawing reasonable liability lines in this context due to uncertain and potentially asymmetrical costs and harms).

[186] *See* Lemley & Reese, *supra* note 5, at 1386–90 (detailing the unworkability of allowing courts or Congress to dictate technological standards to programmers as well as the suppressive effect that liability has on innovation); *see also* Henry H. Perritt, Jr., *Economic and Other Barriers to Electronic Commerce*, 21 U. PA. J. INT'L ECON. L. 563, 563–67, 573–75 (2000) (discussing both economic and regulatory barriers to entry and how they affect the cost of entering markets).

[187] *See* Perritt, *supra* note 186, at 563–67 (describing the effect the internet has had on lowering the barriers to enter global commerce).

current juggernauts of industry, creating a regime that only they can afford to comply with.[188]

The potential benefits that would be foregone by increasing these barriers to entry are inherently speculative, but can be informed by current trends in the industry that demonstrate how data integration can be a competitive advantage.[189] The rise of "smart" devices illustrates the extent that connectivity and data integration now provides a cheap and cost-effective market advantage over unconnected devices.[190] Many of these devices are poorly secured, as evidenced by news reports of hackers infiltrating a wide range of connected devices, including one such instance where the processing power of thousands of smart-fridges was commandeered into a "botnet" army assembled to facilitate further attacks.[191] The cost of securing such products could mean they disappear from the market, forcing policymakers to ask: are Americans better served trading in their smart fridges—or ensuring that all future smart fridges are made by Google and Apple—in favor of security?[192]

The market failures that are incentivizing continued vulnerability suggest that government intervention could increase efficiency by accounting for group interests that individual actors do not prioritize.[193] Some sources draw similari-

---

[188] *See id.* at 565–67 (explaining that the lower barriers to entry mainly benefit smaller entities).

[189] *See* Lemley & Reese, *supra* note 5, at 1386–90 (explaining that the potential harms and benefits of technology are unknowable and uses the VCR and radio as examples of disruptive technologies that eventually came to greatly benefit the industries that initially attempted to suppress them).

[190] *See* SCHNEIER, *supra* note 8, at 5 (attributing the explosive growth of the Internet of Things industry to the perceived competitive edge that connectivity gives over older products). The term "smart" device typically refers to products that are in some way internet-connected and data integrated, a capability that is used in a wide range of products to add control and functionality. *See* Manuel Silverio, *What Is a Smart Device?—The Key Concept of the Internet of Things*, TOWARDS DATA SCI. (Dec. 29, 2019), https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-the-internet-of-things-52da69f6f91b [https://perma.cc/K3R8-S28N] (discussing the core features of smart devices and the various uses of these data integrated products).

[191] *See* SCHNEIER, *supra* note 8, at 1 (titling his introductory chapter, "Everything is Becoming a Computer"); Swapnil Bhartiya, *Your Smart Fridge May Kill You: The Dark Side of IoT*, INFOWORLD (Mar. 3, 2017), https://www.infoworld.com/article/3176673/internet-of-things/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html [https://perma.cc/QJ3L-H2ZH] (explaining the rampant security design flaws in Internet of Things devices); *Is Your Smart Fridge Part of a Criminal Botnet?*, PYMNTS (June 30, 2017), https://www.pymnts.com/news/security-and-risk/2017/watchguard-internet-security-report-shows-your-fridge-could-be-part-of-a-hackers-botnet/ [https://perma.cc/5X3A-TD9C] (reporting on the vulnerabilities that led to the Mirai botnet that allowed the hijacking of smart devices for use in cyberattacks).

[192] *See* Lemley & Reese, *supra* note 5, at 1386–90 (explaining how this cost-benefit analysis involves many uncertain factors); Perritt, *supra* note 186, at 573–75 (discussing the effect of compliance with regulatory barriers to entry on innovation).

[193] *See* Howard C. Kunreuther & Mark V. Pauly, *Behavioral Economics and Insurance: Principles and Solutions*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF INSURANCE LAW, *supra* note 56, at 16–17 (hypothesizing that government intervention is appropriate when anomalous behavior causes the under-purchase of protection or harm to others or when individuals have difficulty reducing their own risk); Shavell, *supra* note 16, at 359–64 (examining the determinants of efficient government intervention); *see also* Shavell, *supra* note 173, at 256–57, 279–81 (explaining how individuals

ties between data breach risk and the risk environments that characterize special insurance programs, like Workers' Compensation, the National Flood Insurance Plan, and health insurance, and make recommendations for a tailored program to suit their perceived needs of the industry or consumers.[194] In an ubiquitous risk environment, such as the ever-present risk of workplace accidents, a centralized response can greatly reduce transaction costs and benefit from economies of scale.[195] Further, such centralized responses are efficient when most victims require similar remedies.[196] The no-fault reimbursement system created by Workers' Compensation statutes consolidates and reduces transaction costs by implementing a remediation process handled by a central authority, eliminating the need to litigate most workplace accidents.[197]

Looking abroad for answers yields little at this moment—the GDPR took effect in May 2018 and there remains a dearth of enforcement actions under its provisions, so its economic impact is not yet fully understood.[198] Commentators at opposite ends of the spectrum have mused that the GDPR will be either functionally limited in application due to enforcement issues or will have a massive impact on the data economy.[199] While regulatory action under the

---

often consider private benefits and not social benefits in decision making and how groups do the opposite).

[194] *See* Kesan & Hayes, *supra* note 9, at 273–76 (noting similar features in cybersecurity to the issues that prompted the National Flood Insurance Program and Workers' Compensation and suggesting a public subsidy for private insurance); Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 416–18 (2016) (likening the needs of the cybersecurity industry to floodplains risks and proposing subsidized and centralized insurance program for organizations to buy into).

[195] *See* Fishback & Kantor, *supra* note 74, at 307, 309 (discussing how transaction costs can be reduced through a prescribed centralized remediation process when the needs of individuals are similar); *see also* Mark A. Lemley & R. Anthony Reese, *A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes*, 23 CARDOZO ARTS & ENT. L.J. 1, 9, 14–15 (2005) (arguing that a centralized and clear remedy in the uncertain area of digital copyright infringement would provide a more efficient response than litigation of novel and complex issues).

[196] *See* Lemley & Reese, *supra* note 5, at 1350–52 (suggesting a centralized dispute resolution system would reduce the cost of enforcement by providing faster remedies than requiring copyright owners to sue infringers or facilitators of infringement).

[197] *See* Fishback & Kantor, *supra* note 74, at 306–10 (explaining the appeal of the Workers' Compensation system to both employers and employees and the benefits of the reduction in transaction costs and the cost certainty created).

[198] *See* DLA PIPER, *supra* note 133, at 3 (reporting the findings of an earlier survey and finding over fifty-nine thousand reported breaches between May 2018 and May 2019). There have been high-profile enforcement actions of other GDPR privacy provisions in recent months, but the survey found only relatively small fines assessed for data breach incidents. *See id.*

[199] *See, e.g.*, Tal Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1018–19 (2017) (forecasting possible outcomes and potential issues with enforcement); Jeremy Kahn et al., *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, BLOOMBERG (Mar. 22, 2018), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law [https://perma.cc/R9ZZ-KE54] (reporting industry opinions on GDPR obligations and forecasting almost $8 billion in compliance costs for large corporations alone); Yves Le Roux, *Could GDPR Shrink Big Data?*, INFOSECURITY MAG. (Aug. 10,

GDPR mostly consisted of minor fines in 2018, a number of more significant fines were levied in 2019, such as the £183 million fine imposed on British Airways following an attack that exposed the information of 500,000 users.[200]

III. GIMME SHELTER: SECURITY AND SMART-FRIDGES

The technology revolution and the accompanying impossibility of cybersecurity have created an economy that carries poorly understood risks.[201] The lack of comprehensive data regulation in the United States has funneled the process of delineating the duties, obligations, and standards to the courts and regulatory bodies.[202] The emergent theme to the largely reactive private and public enforcement of data breaches has been a judicial search for limiting principles that do not cause earthquakes in the status quo.[203] This has resulted in a system that painfully draws out litigation, creates excess costs, and leaves few stakeholders satisfied—while also completely failing to effectively protect data.[204] Imposing new data security requirements could have a huge impact on our economy, but will require a great deal of thought, care, and time to proper-

2017), https://www.infosecurity-magazine.com/opinions/could-gdpr-shrink-big-data/ [https://perma.cc/7G4K-23S8] (discussing the cost of compliance and the implications on the data industry).

[200] *See* DLA PIPER, *supra* note 133, at 3 (examining some of the early and largely minor enforcement actions under the GDPR breach notification rules); *British Airways Faces Record £183m Fine for Data Breach*, BBC (July 8, 2019), https://www.bbc.com/news/business-48905907 [https://perma.cc/W32X-E9NQ] (detailing the record breaking fine against the airliner following a malicious attack that rerouted users to a fraudulent site that collected their information); *Major GDPR Fine Tracker*, *supra* note 133 (reporting on major GDPR fines since the regulation has taken effect).

[201] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 4, 8–9 (discussing the reasons behind systemic cyber insecurity); SCHNEIER, *supra* note 19, at 141 (listing various factors that contribute to the defender's disadvantage in cybersecurity).

[202] *See* Boyne, *supra* note 3, at 299–304, 332–33 (discussing and listing the various industry-specific regulations that apply to data breaches).

[203] *See, e.g.*, Longenecker-Wells v. Benecard Servs., No. 1:15-CV-00422, 2015 WL 5576753, at *16 (M.D. Pa. Sept. 22, 2015) *aff'd*, 658 Fed. App'x 659 (3d Cir. 2016) (describing the difficulty of drawing reasonable liability lines in this context).

[204] *See In re* Zappos.com, Inc., 888 F.3d 1020, 1025 (9th Cir. 2018) (finding that increased risk of identity theft suffices for Article III standing some six years after the cases were filed and consolidated); Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 2–6 (chronicling the consolidated litigation comprising over one hundred filed suits and several hundred claims arising out of the laws of all fifty states and the ensuing settlement negotiations); THE AFTERMATH 2018, *supra* note 33, at 5 (reporting satisfaction levels below 50% for consumer dealings with credit issuers and financial services, credit reporting agencies, law enforcement, and the Federal Trade Commission).

ly implement.[205] Both data subjects and organizations, however, suffer in the interim due to the lack of clear standards.[206]

This Part reexamines current issues with data breach litigation and looks ahead to future issues that may further complicate it and proposes a narrow solution, albeit requiring comprehensive federal legislation.[207] Section A analyzes the reasons why the courts and the system of private liability are ill-suited to the data breach context.[208] Section B argues that a legislatively created consumer remedy for compromised data subjects would reduce costs by eliminating the need for wasteful and complicated consumer data breach class action lawsuits.[209] Section B also argues that a safe-harbor based compliance scheme that facilitates cost-effective cybersecurity strategies would more effectively incentivize organizations to take action by providing greater cost certainty without discouraging innovation.[210]

A. The Courts Are Ill-Equipped to Handle Consumer Data Breach Litigation

It is unlikely the courts can provide an efficient remedy for consumers given the existing roadblocks.[211] Litigating this issue is made difficult by the dynamics of data security and data risk that often yield a large number of data breach victims spread across the country.[212] Litigation is expensive even where the law is settled, but the lack of precedent in this area makes these cases extremely complicated.[213] The lack of consensus on what constitutes reasonable

---

[205] *See* Cortez, *supra* note 180, at 176–77, 182–85 (describing the difficulties created by disruptive innovations on regulatory schemes that fit previous frameworks); Johnson & Post, *supra* note 179, at 1370–76 (discussing the futility of traditional notions of governance due to the lack of borders); Lemley & Reese, *supra* note 5, at 1346–49, 1381–86 (detailing the effects on industries of attempts to regulate novel issues posed by technology).

[206] *See* THE AFTERMATH 2018, *supra* note 33, at 5 (reporting on the considerable consumer dissatisfaction with standard identity theft reimbursement and resolution processes); PONEMON INST., *supra* note 10, at 30 (showing that American organizations face an average cost of $7.91 million following a data breach); Fishback & Kantor, *supra* note 74, at 316 (discussing how unclear legal standards prior to the adoption of Workers' Compensation statutes encouraged more creativity in litigation to test the limits of the precedent, resulting in an increase in lawsuits).

[207] *See infra* notes 211–272 and accompanying text.

[208] *See infra* notes 211–238 and accompanying text.

[209] *See infra* notes 247–253 and accompanying text.

[210] *See infra* notes 254–272 and accompanying text.

[211] *See* Shavell, *supra* note 16, at 366–69 (describing several factors that make private liability a preferable enforcement mechanism over government regulation).

[212] *See id.* at 366–68 (stating that liability is preferable when the risks are easily accounted for, effective precautions exist, and the harms are readily apparent and not dispersed among many victims when they occur).

[213] *See id.* at 368–69 (stating that liability is more efficient when some administrative costs can be avoided by clear legal standards because unnecessary lawsuits will be discouraged when entities are clearly in compliance).

security further complicates the development of a litigable standard.[214] New difficulties litigating data breaches may also emerge in the future considering how prevalent this problem is likely to continue to be.[215]

The multijurisdictional nature of many of these suits introduce novel concepts of law under multiple states' laws simultaneously.[216] Part of the problem is that consumers have no way to seek a remedy by themselves, so they must amass a class as large as possible to increase bargaining power.[217] The battle over Article III standing and whether to include those who have not yet suffered harm is paramount to plaintiffs as well as exceptionally difficult for the courts to handle.[218] The equally unsatisfying alternatives either allow too many plaintiffs into the class and overinflate the projection of harm—and size of the eventual settlement—or require compromised plaintiffs to suffer concrete harm first before seeking redress.[219] The uncertainty around what must be shown at this stage, as well as the potential stakes, often leads to a vigorous challenge from both sides and sometimes multiple interlocutory appeals.[220]

---

[214] *See, e.g.*, LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236–37 (11th Cir. 2018) (discussing the difficulties of litigating reasonable security because of disagreement between experts in the field as to what combination of security measures suffices).

[215] *See* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 696–97 (7th Cir. 2015) (examining issues of tracing causation when multiple breaches happen close in time); Kosseff, *supra* note 194, at 414 (suggesting that the relative speeds of technological advancement and the legislative process will cause some legislative remedies to quickly become obsolete).

[216] *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1172–76 (D. Minn. 2014) (assessing various issues in an action consolidated from thirty-three actions originally filed in eighteen federal districts).

[217] *See* Shavell, *supra* note 173, at 279–80 (discussing how centralized enforcement is preferable in the context of distributed harms by pollution where individuals may lack the incentive to bring suits as individual harms are relatively small). Considering the likely remedy of a settlement could amount to as low as a couple hundred dollars' worth of credit monitoring services and reimbursement of provable losses, it is unlikely to be worth the cost of litigation for any single plaintiff. *See id.* (discussing how high transaction costs may prevent individuals from pursuing legal action when their own individual harm is fairly low). In general, this is the enforcement mechanism that class action lawsuits are supposed to fill, but class certification is not easy in this context due to the issues regarding standing and whether putative future victims will be included in the class. *See* Black, *supra* note 75, at 200–06 (detailing several class action certification difficulties that data breach litigants face); *see also supra* notes 75–93 and accompanying text (discussing the battle for standing in data breach litigation).

[218] *See, e.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020, 1025 (9th Cir. 2018) (finding that Article III standing was met when there was an increased risk of identity theft after the cases had been filed and consolidated about six years later); Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017) (finding that increased future risk of identity theft was sufficient for standing); Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017) (finding increased risk of future identity theft insufficient for standing).

[219] *See Remijas*, 794 F.3d at 693 (opining that plaintiffs should not have to wait to suffer injury in order to satisfy standing or class certification because it was objectively reasonable that such injury would occur).

[220] *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 892 F.3d 968, 979 (8th Cir. 2018) (affirming grant of motion to certify class that was appealed by members of the class who objected to a proposed settlement); *In re* Target Corp. Customer Data Sec. Breach Litig., 847 F.3d 608, 615–16 (8th Cir. 2017) (reversing and remanding for reconsideration of class certification).

Developing a standard to evaluate whether reasonable cybersecurity was implemented in a given case would be complicated by the variability of security practices and budgets of all data-enhanced companies across all industries.[221] Reasonable security as a legal standard would encompass a massive grey area and be largely unprovable shy of clearly superlative security or obvious gross negligence.[222] Given the disagreement between cybersecurity experts, a jury would face significant difficulty accurately determining whether reasonable security was provided.[223]

A reasonable security standard would also fail to achieve perfect protection, and in many cases, reasonable security for a given organization would still result in a highly vulnerable state.[224] Some companies may be able to invest heavily in security, but others may be more hard-pressed to do so, and thus hackers could opportunistically choose targets based on vulnerability.[225] A standard that avoids commandeering the budgets of all data-augmented organizations would guarantee continuing vulnerability and likely provide little protection for data subjects.[226] In cases where a business made reasonable expenditures and was breached nonetheless, went bankrupt as a result of a data breach, or could not otherwise pay for the harm, the compromised data subjects would be left without a remedy.[227]

The lack of consensus as to what constitutes reasonable security prevents tort and contract law from adequately serving the needs of data subjects.[228]

---

[221] *See LabMD, Inc.*, 894 F.3d at 1236–37 (musing on the difficulty of proving reasonable security standards were met); Brief of the National Technology Security Coalition as Amicus Curiae in Support of Petitioner and Vacatur, *supra* note 73, at 17–19 (advocating that rigid standards ignore the practical realities most businesses face, including budget issues, compatibility issues, and the work required to implement changes to a complex IT system).

[222] *See LabMD, Inc.*, 894 F.3d at 1236–37 (discussing the practical limitations to litigating reasonable security due to lack of clear standards and industry consensus); Brief of the National Technology Security Coalition as Amicus Curiae in Support of Petitioner and Vacatur, *supra* note 73, at 5–8 (detailing the complicated cost-benefit analysis that must be undertaken regarding cybersecurity investments and how they differ considerably across organizations).

[223] *See, e.g.*, *LabMD, Inc.*, 894 F.3d at 1236–37 (positing a hypothetical back-and-forth *ad infinitum* between cybersecurity expert witnesses on what constitutes reasonable security).

[224] *See* Selznick & LaMacchia, *supra* note 172, at 244–47 (remarking that reasonable security for many small businesses would only account for minimal precautions).

[225] *See* SCHNEIER, *supra* note 19, at 140–43 (explaining how most cybercrime is opportunistic and targets are chosen based on who is vulnerable to readily accessible methods); Selznick & LaMacchia, *supra* note 172, at 244–47 (discussing budgetary issues that prevent small businesses from investing heavily into cybersecurity).

[226] *See* SCHNEIER, *supra* note 19, at 141–50 (detailing the systemic difficulties of cybersecurity); Selznick & LaMacchia, *supra* note 172, at 244–47 (explaining that small businesses often must prioritize operations over cybersecurity given a limited budget).

[227] *See* Shavell, *supra* note 16, at 360–63, 67 (discussing instances where private liability is less preferable because organizations cannot or are unlikely to pay for the harm caused).

[228] *See id.* at 366–68 (explaining that private enforcement of liability is more efficient when private parties make rational decisions based on the riskiness of their activities, when private parties are

Negligence claims struggle proving duty, breach of that duty, and causation.[229] Established standards of care discourage suits where the standard was clearly met, but such standards will be almost impossible to define in the context of data breaches.[230] Contract clauses guaranteeing reasonable security would also be difficult to litigate due to this lack of consensus.[231] Moreover, attempts to assign fault within the organic network of vulnerabilities that comprise both technological and human nature struggle in this environment.[232] Consumer data would not aggregate to the level where it would be valuable to thieves if consumers were not so willing on an individual level to barter with it.[233] Thus, every member of the data economy bears some level of fault.[234]

The difficulties are likely to get worse as breaches continue to occur and courts will struggle with the additive effects of continuous and overlapping breaches, as well as multiple sources of harm.[235] As technology continues to become more complex, existing reasonable security standards will quickly be-

---

able to pay for the harm done, and when litigation is relatively cheap and includes clear legal standards).

[229] *See LabMD, Inc.*, 894 F.3d at 1236–37 (pondering the practical difficulties that litigating a breach of duty would pose); *Remijas*, 794 F.3d at 696–97 (discussing the standard of causation that must be sufficiently plead for standing purposes); *see also* E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.07 (discussing state common law claims and litigation of duties, breaches of that duty, causation, and harm). Both of these are largely untested standards beyond the most preliminary stages of litigation. *See LabMD, Inc.*, 894 F.3d at 1236–37; *Remijas*, 794 F.3d at 696–97.

[230] *See* Shavell, *supra* note 16, at 368–70 (explaining that the administrative costs attendant to determining compliance bear in favor of public regulation when large amounts of institutional knowledge is required to keep these costs low); *see also* Brief of the National Technology Security Coalition as Amicus Curiae in Support of Petitioner and Vacatur, *supra* note 73, at 13 (detailing the challenge CISOs face in keeping up with constantly evolving threats and the considerable resources this requires).

[231] *See* SCHNEIER, *supra* note 8, at 133–34 (explaining how consumers have no practical way of determining whether companies are representing their security procedures accurately); Strahilevitz & Kugler, *supra* note 168, at 92 (stating that consumers cannot understand most terms of use clauses); *see also LabMD, Inc.*, 894 F.3d at 1236–37 (remarking on the difficulties of litigating a cybersecurity technical standard); E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.10 (discussing contractual security provisions and litigation).

[232] *See* Kesan & Hayes, *supra* note 9, at 220–21 (stating that externalities are pervasive in cybersecurity due to cost spreading); Shavell, *supra* note 145, at 203–04 (explaining how employee decisionmakers do not face the same incentive to prevent harm to the organization because they will not experience the majority of this harm).

[233] *See* SCHNEIER, *supra* note 19, at 53–56 (providing examples of how deep collections of data spur better personalized advertising through complicated algorithms that in turn increases the value of data collection efforts); Shavell, *supra* note 173, at 256–57 (explaining how individuals discount social benefits in their own decision making).

[234] *See supra* note 233 and accompanying text.

[235] *See Remijas*, 794 F.3d at 696–97 (discussing issues of causation when multiple breaches happen within a short time-frame); *Data Breaches*, *supra* note 7 (compiling reported breach figures since 2005); *ITRC Multi-Year Data Breach Chart*, *supra* note 7 (graphing the increase from 157 reported breaches in 2005 to over one thousand reported breaches in each of the past three years).

come obsolete.[236] Causation could become more difficult to prove if the breached data could have originated from any number of breach points.[237] It could get even harder for courts to draw the line between granting costly e-discovery to bear out such allegations to too many plaintiff classes or too few.[238]

B. Embracing Insecurity: Harm Reduction and Cost-Efficiency

It is beyond the scope of this Note to propose anything more than a basic framework for what will inevitably be one of the most complicated pieces of legislation in recent history.[239] The question of how this activity would be funded is also beyond the scope of this Note, but the centralization of both the remedy and enforcement mechanism should provide significant cost savings overall to both industry and the citizenry.[240]

---

[236] *See* Brief of the National Technology Security Coalition as Amicus Curiae in Support of Petitioner and Vacatur, *supra* note 73, at 17–19 (advocating that strict technical standards would be difficult to keep up with and require constant investment in attempts to comply). The constant evolution of technology presents major challenges to cybersecurity as the nature of cyber threats evolves at a similarly rapid pace and requires that chief information security officers "plan and re-plan for an overwhelming number of contingencies." *Id.* at 13.

[237] *See Remijas*, 794 F.3d at 696–97 (finding that causation was sufficiently alleged at the pleading stage despite multiple breaches occurring at roughly the same time). The court cited a landmark joint liability case involving a plaintiff who was shot by two defendants at the same time. *Id.* at 696 (citing Summers v. Tice, 192 P.2d 1, 5 (Cal. 1948)). When two potential sources of the harm exist, the burden falls to the defendant to prove that they were not the "but-for" cause of the injury. *Id.* Now, imagine that hundreds of breaches have occurred close in time and targeted similar demographics—this could create quite a burden on breached organizations trying to prove it was not *their* breach that caused the harm. *See id.* Courts may even face the challenge of determining whether the repeated breach of data begins to dilute its value—if the data has been compromised several times already, how much more harmful are subsequent breaches? *See* SCHNEIER, *supra* note 8, at 130 (discussing how difficult it may be to prove a breach caused harm when the compromised data was already available for sale on the black market).

[238] *See* Grigsby v. Valve Corp., No. C12-0553JLR, 2012 WL 5993755, at *4 (W.D. Wash. Nov. 14, 2012) (dismissing the complaint and referencing the higher threshold that must be plead over standard torts in consideration of the costly e-discovery that would commence); Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 1–6 (mentioning the discovery process thus far in the streamlined litigation, including over two hundred depositions, fourteen discovery motions, and almost four million pages of documents).

[239] *See infra* notes 247–272 and accompanying text (proposing the framework of a socially optimal solution).

[240] *See supra* notes 1–238 and accompanying text (providing background and discussing and analyzing why the attempts to outline a workable private liability standard have failed and created excess costs); *infra* notes 247–272 and accompanying text (discussing why a no-fault approach would reduce costs primarily by consolidating transaction and administrative costs); *see also* Victoria Graham, *Dem Presidential Candidates Seize on Antitrust as Campaign Issue (1)*, BLOOMBERGLAW (Mar. 11, 2019), https://news.bloomberglaw.com/mergers-and-antitrust/dem-presidential-candidates-seize-on-antitrust-as-campaign-issue-1 [https://perma.cc/8UTG-RPRH] (discussing Senator Amy Klobuchar's informal proposal to tax tech companies for the use of large consumer datasets). Senator Klobuchar's proposal echoes a similar proposal made by the European Commission to establish a 3% digital services tax on large corporations applicable to revenues resulting from the use of consumer data. *See Commission Proposal for a Council Directive on the Common System of a Digital Services Tax on*

The economic principles and technical difficulties surrounding this issue indicate that Congress should create a centralized remedy similar to the no-fault Workers' Compensation reimbursement scheme in order to reduce the costs and harms of data breach.[241] A limited approach that both creates a consumer remedy and a regulatory authority to govern all data breach matters would improve outcomes for both consumers and organizations.[242] The creation of a National Fund for Identity Theft will provide data subjects with direct redress for their harms and reduce transaction costs and administrative fees.[243] The empowerment of a regulatory body and the creation of a safe-harbor based incentive scheme will hold organizations more accountable and provide them with cost certainty and elimination of catastrophic data breach risk.[244]

Most importantly, this proposed solution is narrow enough in scope that it can act as a remedy in the near-term for consumers facing identity theft issues while the debates on greater issues of cybersecurity, national security, and the future of technology continue to coalesce.[245] Perhaps providing data subjects

---

Revenues Resulting from the Provision of Certain Digital Services, at 24–28, COM (2018) 148 final (Mar. 23, 2018) (discussing the European Commission's tax); Graham, *supra* (discussing Senator Klobuchar's tax).

[241] *See* Fishback & Kantor, *supra* note 74, at 309 (explaining how Workers' Compensation statutes were of benefit to both employers and employees because they reduced the cost of settling frequent workplace accident claims); *see also supra* notes 18–63 and accompanying text (discussing the costs of data breach).

[242] *See* Steven Shavell, *Risk Aversion and the Desirability of Attenuated Legal Change*, 16 AM. L. & ECON. REV. 366, 393–95 (2014) (discussing how the speed of desirable legal change for each stakeholder depends on their cost-benefit analysis of the increased compliance costs and increased benefits of the change). The only stakeholders that would stand to lose in this approach is the Data Breach Plaintiff's Bar and the firms retained by the breached organizations, who have reaped considerable benefits from the uncertain legal standards. *See id.*; *e.g.*, *In re* Yahoo! Inc. Customer Data Security Breach Litig., No. 16-MD-02752-LHK, 2019 WL 387322, at *13–21 (N.D. Cal. Jan. 30, 2019) (denying the proposed settlement in part because the court concluded that the proposed $35 million set aside for attorney's fees was excessive in light of the relatively minimal litigation work done by the class representatives).

[243] *See* Fishback & Kantor, *supra* note 74, at 309 (explaining that the centralized Workers' Compensation dispute resolution scheme created an efficient claim process by consolidating administrative costs and obviating complicated litigation).

[244] *See* Kosseff, *supra* note 194, at 412–14 (discussing a safe-harbor incentive for data security); Lemley, *supra* note 17, at 119 (finding that the safe-harbor enforcement method is an optimal enforcement mechanism for internet intermediaries).

[245] *See* DANIEL R. COATS, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 5 (Feb. 13, 2018) (listing cyber threats first among global threats and warning of sophisticated acts by state actors as well as lesser criminal acts). Security by design has been embraced as a key goal for future development of connected products. *See, e.g.*, TIMOTHY E. LEVIN ET AL., SECURECORE, DESIGN PRINCIPLES AND GUIDELINES FOR SECURITY 1–2 (2007) (discussing the importance of emphasizing security at the design stage of a new product). This becomes practically difficult due to the Lemons Market effect resulting from consumer tastes and preferences rarely rewarding such investment. SCHNEIER, *supra* note 8, at 133–35. Such solutions, should the Lemons Market roadblock be overcome, are necessarily forward thinking and would require an overhaul of the systems and programs we currently rely on. *See* N.Y. CYBER TASK

with a reliable and easy remedy will also reduce the taboo of data breach—significant reputational harm and damage-control costs could be avoided if the inevitability of insecurity and its harms are recognized and accounted for.[246]

1. Consumer Remedy

Establishing a National Fund for Identity Theft will substantially simplify the process of seeking redress for identity theft issues.[247] Quite similar to how Worker's Compensation funds work, the ubiquitous risk can be more efficiently accounted for by the reduced transaction costs and the economies of scale that a centralized response provides.[248] This would allow individuals to seek reimbursement or credit monitoring when it is *actually* needed and it is likely to provide a more satisfactory resolution process.[249] The required disclosures and compliance obligations of the safe-harbor program detailed below will help create a more efficient response through information sharing and potentially affected individuals can be more quickly alerted and monitored.[250]

This remedy removes the need for data subjects to attempt to litigate reasonable security standards, class certification, or standing.[251] It eliminates the

---

FORCE, *supra* note 6, at 22–23 (making recommendations for future development of a more defensible cyberspace). Minimizing the complexity of computer networks by reducing the number of unique programs and software is one such recommendation to shift the balance in favor of defenders by reducing the number of potential vulnerabilities that must be accounted for. *Id.*

[246] *See* DREYER ET AL., *supra* note 11, at 1 (finding reputational losses account for 8% of the costs of data breaches to organizations); PONEMON INST., *supra* note 10, at 29 (finding that American organizations face higher costs due to customer loss and diminished goodwill than other countries); *see also supra* notes 137–178 (discussing the guaranteed insecurity of internet connected devices).

[247] *See, e.g.*, *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1172–76 (analyzing the precedents of eleven different states in order to determine which plaintiffs will be included in the large federal plaintiff class); Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 1–6 (recounting the history of the litigation, consolidated into a single action from over one hundred lawsuits and several hundred claims under all fifty state laws and including considerable discovery efforts and over a dozen motions).

[248] *See* Kesan & Hayes, *supra* note 9, at 269–76 (noting similar features in cybersecurity to the issues with inefficient transaction costs that prompted the National Flood Insurance Program and Workers' Compensation and suggesting a public subsidy for private insurance).

[249] *See Remijas*, 794 F.3d at 693 (remarking that the plaintiffs who have not yet suffered harm should not have to wait until they do to seek redress); THE AFTERMATH 2018, *supra* note 33, at 5 (discussing consumer satisfaction with identity theft resolution processes); THE AFTERMATH 2017, *supra* note 11, at 7–12 (discussing the negative impacts of identity theft).

[250] *See* Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 259–60 (2011) (finding a 6.1% reduction in identity theft following timely breach notifications in a survey of the beneficial effects that predated the mass adoption of such laws). Breach notification helps those affected avoid harm if proactive measures, such as credit freezes or credit monitoring, are undertaken to prevent potential identity theft. *See id.*

[251] *See* Fishback & Kantor, *supra* note 74, at 307, 316 (discussing the benefits to both employers and employees of removing the need to litigate workplace accidents, an area governed at the time by uncertain legal standards and defenses that prompted excess litigation); *see also supra* notes 64–133

difficulty of granting too many or too few plaintiffs standing and reduces waste in the form of settlement funds earmarked for potential future victims who may not actually suffer harm.[252] It will benefit organizations by reducing the forecasted risk of a breach and removing the considerable costs of data subject litigation, allowing them to focus on the other litigation they are likely to face.[253]

2. Incentives-Based Regulation of Data Security

An incentives-based regime that provides a safe-harbor from consumer data breach litigation will allow organizations to operate with more cost certainty and can be leveraged to promote better practices throughout the industry.[254] This greater cost certainty and overall clearer compliance standards should help foster innovation rather than restrict it.[255] Avoiding consumer data breach litigation, and thus reducing the costs and risks of a potential data breach, will be a far more effective incentive to meet compliance standards.[256]

Data breaches would not go entirely unpunished and the regulatory authority could assess fines or other heightened compliance requirements.[257] These fines would be more appropriately tailored to the actual harms of a data breach and would be far less expensive than litigating a data breach by elimi-

---

and accompanying text (providing background information on the various difficulties of consumer data breach litigation).

[252] *See, e.g.*, *Remijas*, 794 F.3d at 693 (deciding that a potentially larger than necessary class was more fair than requiring consumers to actually suffer harm before seeking redress); *In re Yahoo! Inc. Customer Data Security Breach Litig.*, 2019 WL 387322, at *22 (denying the proposed settlement agreement in part due to the potentially inflated number of class members in comparison to the number of active Yahoo! users at the time).

[253] *See* PONEMON INST., *supra* note 10, at 28 (reporting the significant costs of litigation to breached organizations); *supra* notes 60–63 and accompanying text (discussing the complex business-to-business litigation that often follow data breaches).

[254] *See* Kosseff, *supra* note 194, at 412–14 (arguing that incentive-based safe-harbor programs achieve greater compliance by offering organizations an optional compliance regime that creates cost certainty).

[255] *See* Stephen Shavell, *Do Excessive Legal Standards Discourage Desirable Activity?*, 95 ECON. LETTERS 394, 395 (2007) (modeling a depressive effect on innovation if the legal standard is overly burdensome). This should not be an issue here, as theoretically the costs of a data breach will be reduced overall and costs of precautions will be clarified. *See id.*

[256] *See* PONEMON INST., *supra* note 10, at 28 (reporting on the considerable litigation costs of data breaches that American organizations incur); Fishback & Kantor, *supra* note 74, at 306–10 (detailing the appeal of the no-fault system to employers, who saved on the considerable transaction costs of litigating workplace accidents); Shavell, *supra* note 173, at 279–80 (explaining scenarios where organizations are unlikely to be motivated to reduce risks if the risky behavior otherwise generates value).

[257] *See* Shavell, *supra* note 16, at 373–74 (comparing the deterrence effect of fines with that of private liability); Shavell, *supra* note 173, at 281 (discussing the effectiveness of fines as an enforcement mechanism in safety regulation when such fines reflect the savings of failing to take required precautions). Shavell writes that fines are sometimes less effective than liability if private parties know when they have been harmed better than public agencies do, but this would be mitigated to some extent by the breach reporting requirements of the safe-harbor. *See* Shavell, *supra* note 16, at 373–74.

nating many of the unnecessary transaction costs.[258] The tiered safe-harbor could offer various levels of protection from these fines in the wake of breach.[259] The highest compliance levels would be akin to some of the auditing and monitoring obligations commonly found in FTC consent decrees and offer complete immunity from fines.[260] Fines would be steep for entities that do not meet the safe-harbor, but increasing levels of compliance activity would yield smaller fines and less exposure to risk.[261] Fines would be based on the amount and the sensitivity of the data lost, which would encourage greater compliance from those using the most sensitive data.[262] This would also encourage organizations to assess what data is actually adding value to their operations and to minimize unnecessary collection.[263] Organizations will be better able to prioritize which of their systems they most need to protect, such as those containing trade secrets or especially sensitive personal data, with this enhanced risk certainty.[264]

The development of institutional knowledge on cybersecurity is crucial to the cost-effectiveness of this model as the information collection will allow for more efficient investments to be made into security.[265] Much of the current

---

[258] *See* A. Mitchell Polinsky & Steven Shavell, *Costly Litigation and Optimal Damages*, 37 INT'L REV. L. & ECON. 86, 86 (2014) (discussing the social costs of complex litigation in addition to the cost of the injury being litigated).

[259] *See* Lemley, *supra* note 17, at 110–19 (exploring the merits and demerits of various safe-harbor frameworks).

[260] *See, e.g.*, Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement, *supra* note 2, at 7 (listing Anthem's three-year auditing and reporting obligations to the plaintiff class of consumers); E-COMMERCE AND INTERNET LAW, *supra* note 4, § 27.06 (listing several Federal Trade Commission consent decrees related to cybersecurity failings); Resolution Agreement between Anthem, Inc. and Dep't of Health and Human Servs. (Oct. 15, 2018) (obligating Anthem to pay $16 million to the U.S. Department of Health and Human Services Office for Civil Rights and to implement a corrective action plan subject to audit for two years).

[261] *See* Kosseff, *supra* note 194, at 412–14 (arguing that incentive-based safe-harbor programs achieve greater compliance by offering organizations an optional compliance regime that creates cost certainty). Greater compliance can be undertaken for greater cost certainty, whereas those that choose a lower level of compliance forego such certainty. *See id.*

[262] *See* Shavell, *supra* note 16, at 373–74 (describing the use of fines as a deterrence method in a regulatory scheme); Shavell, *supra* note 173, at 281–82 (discussing the use of fines as an enforcement mechanism in safety regulations).

[263] *See* Shavell, *supra* note 16, at 373–74 (discussing the deterrence value of fines); Shavell, *supra* note 173, at 281–82 (same).

[264] *See* Gene Fredriksen, *Protecting the Crown Jewels*, FORBES (Aug. 13, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/13/protecting-the-crown-jewels/#42521881a5a9 [https://perma.cc/Q2GX-F4AW] (emphasizing the importance of prioritizing security investment and training to protect against existential data risks); *Cybersecurity Breach Bankruptcy: It Does Happen*, FRACTIONAL CISO (Jan. 23, 2019), https://fractionalciso.com/cybersecurity-breach-bankruptcy/ [https://fractionalciso.com/cybersecurity-breach-bankruptcy/] (explaining the relative risks to businesses of different cyber incidents and listing instances where theft of intellectual property led to bankruptcies).

[265] *See* Shavell, *supra* note 16, at 369 (discussing how regulatory agencies sometimes have an economic advantage over private parties when collection of information requires expensive empirical analysis and aggregation of data). *See generally* DEP'T OF HOMELAND SEC., CYBER INCIDENT DATA AND ANALYSIS REPOSITORY WORKSHOP (2016) (outlining the goals of the Cyber Incident Data and

investment in cyber security is incurred in an inefficient manner across the economy: moderately secure safeguards being deployed at great expense by individual organizations while consumers are still vulnerable from many other angles.[266] Cybersecurity investments are a cost of doing business for responsible organizations, but they do not appreciably increase overall consumer data privacy nor are they likely to prevent costly litigation.[267] The regulatory authority would be directed to propagate cheap and effective practices in a manner similar to the Department of Homeland Security's current Cyber Information Sharing and Collaboration Program.[268]

Breach reporting will be a necessary compliance obligation of the safe-harbor which will encourage timely disclosures.[269] An effective information network can be created and the industry can be alerted to vulnerabilities and hotfixes faster.[270] Reporting will become centralized and more thorough and victims can be more efficiently alerted by the regulatory authority.[271] The compliance scheme could also help outline a workable standard to simplify

---

Analysis Repository (CIDAR), an information collection and dissemination system that seeks to provide timely warnings of cyber threats and direct organizations to patches and hotfixes).

[266] *See* N.Y. CYBER TASK FORCE, *supra* note 6, at 7 (explaining that annual cybersecurity spending has surpassed $75 billion, but has done "little more than slow th[e] progressive onslaught," of cyberattacks). If one company invests enough to secure its systems it is likely to escape harm, but consumers must rely on a near perfect track record among all of the many entities that hold their data. *See* Schneier, *supra* note 169 (describing the scope of the data broker industry and how consumers are largely unaware of how many entities hold their data and how securely it is being held). One such entity failing to do so may compromise data despite all of the money invested by the others. *See id.*

[267] *See* SCHNEIER, *supra* note 8, at 101 ("[S]ecurity is a tax on the honest."); Hermalin, *supra* note 139, at 321 (explaining that the welfare loss is borne by providers of high-quality products in a lemons market when buyers are quality-indifferent).

[268] *See Cyber Information Sharing and Collaboration Program (CISCP)*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp [https://perma.cc/CN5V-SFKM] (detailing the Department of Homeland Security's (DHS) information sharing program, a public-private partnership that helps facilitate information sharing and threat advisories). The Cyber Information Sharing and Collaboration Program is free to join and provides free consulting and security products. *Id.*

[269] *See* Kosseff, *supra* note 194, at 412–14 (discussing the effectiveness of safe-harbors as a compliance incentive given the costs and uncertainties associated with litigation).

[270] *See National Cybersecurity and Communications Integration Center*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center [https://perma.cc/2UK2-XE9A] (detailing the DHS information sharing program, the National Cybersecurity & Communications Integration Center (NCCIC)); *see also* DEP'T OF HOMELAND SEC., *supra* note 265 (emphasizing the importance of data collection through the creation of the CIDAR database of information surrounding cyber incidents). NCCIC, CIDAR, and other information sharing programs seek to collect and distribute information and provide alert systems that will help security professionals react to new threats faster and reduce the harm caused by each threat. *See* DEP'T OF HOMELAND SEC., *supra* note 265; *National Cybersecurity and Communications Integration Center*, *supra*.

[271] *See Breach Notification Laws*, *supra* note 56 (listing the state breach notification laws for all fifty states). Breach notification has clearly been identified as an important feature of any data security law. *See id.*; *see also* Romanosky et al., *supra* note 250, at 259–60 (discussing how timely breach notification allows potential victims to take protective measures prior to experiencing harm).

some of the litigation that it does not obviate, like contract and indemnification claims between businesses.[272]

CONCLUSION

Consumer data breach litigation encounters numerous roadblocks that hinder efficient resolutions and often requires years of litigation before consumers receive a remedy for their harms. The unique risk environment created by the risk uncertainty, market failures preventing consumers and organizations from properly valuing security, and the inherent vulnerability of technology create considerable excess costs in this litigation. The extension of liability in this area could have far-reaching effects on the development of many data integrated technologies and industries. Significant costs can be saved by ceasing attempts to slowly outline private liability and creating a centralized remedy and enforcement mechanism that acknowledges the inevitability of data breaches and takes advantage of economies of scale. This approach will substantially improve outcomes for both compromised data subjects as well as breached organizations. Additionally, the safe-harbor incentive can be leveraged to improve cybersecurity practices without overburdening data-based innovation.

MAX MEGLIO

[272] *See* Shavell, *supra* note 16, at 369 (describing how regulatory agencies can have an advantage over private parties due to economies of scale when collection of information requires expensive empirical analysis and aggregation of data). *See generally National Cybersecurity and Communications Integration Center*, *supra* note 270 (outlining the goals of the NCCIC information collection and sharing system).