LIABILITY FOR DATA INJURIES

*Jay P. Kesan**
*Carol M. Hayes***

Data insecurity affects the general public to a significant degree, and the law needs to step forward and cope with the challenges posed by data breaches, data misuse, and data injuries. The primary goal of this Article is to provide a thorough analytical framework for data breach cases that specifically focuses on the evolutions needed in the areas of duty and injury in shaping the contours of liability for data injuries. This Article represents the first comprehensive analysis of a duty to secure data within the modern context of data insecurity. While most of our focus is on data breaches, the principles explored in this Article are broad enough to be applied helpfully in data misuse cases as well, including the recent controversy over Facebook's permissive data use practices.

We examine duty as a part of a negligence framework for data insecurity harms, and we argue that courts should recognize a legal duty to secure data. This duty is made necessary by pervasive cognitive biases that result in systematic underestimation of cyber risk by firms and individuals and interfere with the risk management process. A legal duty to secure data is also supported by statutory trends towards liability for people who were upstream or downstream of a data thief.

We also analyze data injuries. Courts struggle with fitting data insecurity injuries within the existing legal models, but part of the reason for that is the preoccupation with economic harm, which is a poor method for quantifying privacy injuries. The erosion of privacy through neglect of security is troubling, and the legal system must shift away from traditional economic measurements of injury and focus instead on the fact that data insecurity is a social harm. Data insecurity is both a privacy injury and an injury to autonomy that interferes with self-determination, and it should be analyzed as such. Our Article represents another step forward in the process of aligning legal protections with the societal shifts driven by technological changes.

* Professor and H. Ross & Helen Workman Research Scholar, University of Illinois. Project Leader, Critical Infrastructure Resilience Institute ("CIRI"), DHS S&T Center of Excellence, University of Illinois.

** Research Associate, Critical Infrastructure Resilience Institute, University of Illinois.

We are grateful to our CIRI colleagues for their insightful comments and suggestions, particularly Linfeng Zhang and Prof. Sachin Shetty.

TABLE OF CONTENTS

I. INTRODUCTION

The last twenty years have seen a lot of change, especially with the rising popularity of the Internet. Modern technology creates challenges and opportunities.[1] As more of our lives went online, we learned the various ways that the law needed to be tweaked or reworked to function in this new dimension of ex-

1. Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 1 (2009) (discussing technology developments in the context of trade secrets).

istence. The Internet is like the planet Crait in The Last Jedi, where the endless salt flats change from white to red with each step.[2] On the Internet, each bit of information that we add paints the landscape, and each step we take leaves data prints.

As the economy of the United States became more centered on electronic exchange, the security risks grew.[3] Discussions of these technological and social evolutions often are pessimistic, and many of the predictions have not come to pass. In 2005, Rustad and Koenig argued that trust is essential to social and commercial relationships, and that rampant cybercrime would create a Wild West of lawlessness and make it difficult to use the Internet for business.[4] Considering the healthy state of e-commerce in 2018, obviously that prophecy misses some marks. They were, however, correct about the lack of trust between consumers and data holders, which has fueled the growth of data breach litigation. In this high risk, low trust environment, the law is one possible tool available to improve these dynamics.

The potential injuries from electronic interference are expansive. In recent years, the world has seen blackouts caused by malware,[5] internet outages caused by botnets,[6] and maybe even the start of a new Cyber Cold War.[7] This Article primarily focuses on data insecurity and especially data breaches. There have been advances in these areas recently, as in February 2018, when the Department of Justice announced a takedown of a major cybercrime ring.[8] The focus was Infraud, a massive cybercrime discussion forum that facilitated the sale of personal data like social security numbers and passwords.[9]

Data breaches follow a familiar pattern. During the 2013 holiday shopping season, the big-box retailer Target was the victim of a massive data breach when hackers absconded with the payment card data for over forty million customers.[10] In a dynamic that is often witnessed, the weakest link caused the data

2. Maddie Stone, *The Amazing Earth Science Behind The Last Jedi's New Mineral World*, EARTHER (Dec. 20, 2017, 10:40 AM), https://earther.com/the-amazing-earth-science-behind-the-last-jedis-new-min-1821429894; THE LAST JEDI (Lucasfilm 2017).

3. Michael D. Simpson, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 669, 674 (2016).

4. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1611 (2005) [hereinafter Rustad & Koenig, *Cybercrime*].

5. *Ukraine Power Distributor Plans Cyber Defense System For $20 Million*, REUTERS (Feb. 6, 2018, 6:58 AM), https://www.reuters.com/article/us-ukraine-cyber-ukrenergo/ukraine-power-distributor-plans-cyber-defense-system-for-20-million-idUSKBN1FQ1TD.

6. Bruce Schneier, *Lessons from the Dyn DDoS Attack, Schneier on Security* (Nov. 8, 2016, 6:25 AM), https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.

7. Rick Noack, *The Dutch Were a Secret Ally in War Against Russian Hackers, Local Media Reveal*, WASH. POST (Jan. 26, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/?utm_term=.c20fc2ddda51. Thanks to AIVD, the Dutch intelligence service, the U.S. intelligence community had access to information about the activities of the Russian hacking group Cozy Bear, which is alleged to have ties to the Russian government. *Id.*

8. Sarah N. Lynch, *U.S. Shuts Down Cyber Crime Ring Launched By Ukrainian*, REUTERS (Feb. 7, 2018, 11:15 AM), https://www.reuters.com/article/us-usa-cybercrime/u-s-shuts-down-cyber-crime-ring-launched-by-ukrainian-idUSKBN1FR2M7.

9. *Id.*

10. Simpson, *supra* note 3, at 671.

breach. In Target's case, the weakest link was a small HVAC vendor with insecure systems.[11] Hackers targeted this vendor with a phishing attack to obtain login information for Target's systems, and then poked at the insecurities within Target's system until they had identified an entry point into Target's payment information files.[12]

In September 2017, the media reported on the potentially most impactful data breach to date, when Equifax disclosed the theft of records associated with 143 million American consumers.[13] Equifax is not a standard consumer-facing company but is instead one of the largest credit reporting agencies in the United States, and its customers include financial institutions that want to know how credit-worthy a particular applicant is.[14] A compromise of that data, with no way to know if any of the stored records were altered, could lead to massive rates of identity theft and harm consumers' ability to obtain credit for major purchases. Such data breaches are a danger to the secrecy of data, but also increasingly to the integrity of data as well. These dangers cause the injury that we refer to in this Article as data insecurity.

Data insecurity manifests significantly in cases of data breaches, but also in cases of data misuse. Data misuse may involve scraping, for example, where someone uses legitimate access to obtain a large amount of data to be used for other purposes, often of a commercial nature. Millions of people use Facebook every day, but in the past, third-party services routinely violated Facebook policies about harvesting user data.[15]

A recent example of data misuse concerning Facebook content is the controversy surrounding Cambridge Analytica and the use of social media information to manipulate political discourse. In the case of Cambridge Analytica, it was revealed that the company used psychographic data profiles to tailor political advertisements, and these profiles were developed in part from data harvested from Facebook profiles.[16]

Some of the more dramatic language about Cambridge Analytica frames its business practice as part of psyops—psychological operations.[17] The revelations about Cambridge Analytica have caused discomfort for many people, perhaps in reaction to the deterministic implications. In a culture that places a

11. *Id.* at 678.

12. *Id.*

13. Patrick Rucker, *Exclusive: U.S. Consumer Protection Official Puts Equifax Probe on Ice–Sources*, REUTERS (Feb. 4, 2018, 12:14 AM), https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ.

14. *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMMISSION CONSUMER INFORMATION (Sep. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

15. Paul Lewis, *'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting Was Routine*, GUARDIAN (Mar. 20, 2018, 7:46 AM), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

16. Angela Chen & Alessandra Potenza, *Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit for Trump*, VERGE (Mar. 20, 2018, 8:00 AM), https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting.

17. *Id.*

high value on individuality, people are especially fearful of being manipulated. Arguably, this fear of manipulation stems from a desire to be the masters of our own fate. This fear ties into a theme that we will revisit in Part IV: injuries to autonomy.

This is not to say that data insecurity is the worst crisis of our time. But it is an important problem that needs to be fixed. Data breaches as a cause of data insecurity are important, but commentary has struggled to reach a balance. The headlines are written to draw attention. Jimmy Koo of Bloomberg declared 2017 to be the Year of the Data Breach.[18] Coincidentally, that has been true of ten of the last twelve years according to a hyperbole-weary cybersecurity blogger.[19] Some have opted to just go ahead and refer to our current time period as "the [d]ecade of the [d]ata [b]reach."[20]

After a major data breach, cybersecurity commentary often includes an unspoken question: Will this be the one? Will this incident be the one that leads to real action? Will lawmakers finally take decisive steps to reduce these risks? Will courts see the incident as an indication that the common law must evolve to address computer-enabled risks and harms? In the year since the disclosure of the Equifax breach, Congress has not taken action. The head of the Consumer Financial Protection Bureau ("CFPB") canceled a probe of the Equifax breach that was initiated by the previous agency head.[21] The Federal Trade Commission ("FTC") is still investigating Equifax, but the FTC's authority is broad and includes many other consumer protection issues as well.[22]

The Equifax data breach affected 143 million people in a country of 250 million adults.[23] In May 2018, Congress enacted the Economic Growth, Regulatory Relief, and Consumer Protection Act.[24] As a result, credit reporting agencies are now required to provide free credit freezes to consumers, including minors.[25] Prior to the Act going into effect, only a few states required credit freezes to be provided for free,[26] so consumers in most states incurred fees to freeze their credit after a data breach. Broader legislative solutions do not seem to be forthcoming, and other government agencies have limited authority and capacity. In a legislative bottleneck like this, courts are essential for helping in-

18. Jimmy H. Koo, *2017: The Year of the Data Breach*, BLOOMBERG BNA (Dec. 19, 2017), https://www.bna.com/2017-year-data-b73014473359/.

19. Tony Martin-Vegue, *Will the Real "Year of the Data Breach" Please Stand Up?*, HACKERNOON (Jan. 4, 2018), https://hackernoon.com/will-the-real-year-of-the-data-breach-please-stand-up-744ab6f63615.

20. Thomas Martecchini, Note, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After* Clapper v. Amnesty International USA, 114 MICH. L. REV. 1471, 1473 (2016).

21. Rucker, *supra* note 13.

22. *See id.*

23. *See id.*; U.S. CENSUS BUREAU, QUICKFACTS, https://www.census.gov/quickfacts/fact/table/US/PST045217 (last visited Nov. 2, 2018).

24. Economic Growth, Regulatory Relief, and Consumer Protection Act, Pub. L. No. 115-174, 132 Stat. 1296 (2018).

25. *See id.*

26. *E.g.*, IDAHO CODE § 28-52-106 (2018) (only requiring credit freezes to be provided at no cost to consumers who are victims of identity theft); N.C. GEN. STAT. § 75-63(o) (2017) (prohibiting fees for credit freezes when the request is made electronically).

jured parties. The current legal environment would greatly benefit from an evolved common law.

Some critics are concerned about relying too much on litigation to address data breaches because of the almost limitless liability that could follow, potentially leading to companies declaring bankruptcy.[27] Riedy and Hanus stop just short of saying that data breach lawsuits are a waste of time and money,[28] and quickly dismiss the argument that litigation is necessary to create incentives for improving security.[29] Romanosky's research team acknowledges the need for balance in litigation.[30] If the litigation model is too weak, harmful and negligent behavior will be undeterred. Heavy-handed use of litigation, on the other hand, might have unintended consequences for innovation.[31] Studies have noted that compared to other countries, one contributor to the higher cost of data breaches in the United States is the higher cost of complying with post-breach regulatory requirements like customer notification.[32]

Data insecurity affects the general public to a significant degree, and the law needs to step forward and cope with the challenges posed by data breaches, data misuse, and data injuries. The primary goal of this Article is to provide a thorough analytical framework for data breach cases that specifically focuses on the evolutions needed in the areas of duty and injury in shaping the contours of liability for data injuries. This Article also represents the first comprehensive analysis of a duty to secure data within the modern context of data insecurity. While most of our focus is on data breaches, the principles explored in this Article may also be applied helpfully in data misuse cases as well, including the recent controversy over Facebook's permissive data use practices.[33]

In Part II, we examine the nature of data misuse and data breaches as well as how that nature contributes to data insecurity. In Part III, we examine duty as a part of a negligence framework for data insecurity harms. We argue that courts should recognize a legal duty to secure data. This duty is supported by legislative trends and is made necessary by pervasive cognitive biases that interfere with the risk management process. In Part IV, we examine data injuries and the possible remedies for those injuries. Courts struggle with fitting data insecurity injuries within the existing legal models, but part of the reason for that is the preoccupation with economic harm. Data insecurity is a privacy injury and an injury to autonomy that interferes with self-determination, and it

27. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 781 (2018); *see also* Dov Fox & Alex Stein, *Dualism and Doctrine*, 90 IND. L.J. 975, 991 (2015) (noting that claim screening mechanisms "operate in order to prevent excessive liability for accidental harm.").

28. Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data Is at Risk: Get Over It!*, 19 SMU SCI. & TECH. L. REV. 3, 6 (2016).

29. *Id.* at 33.

30. Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 75 (2014).

31. *Id.*

32. PONEMON INST., 2017 COST OF DATA BREACH STUDY 3 (2017).

33. *See, e.g.*, Lewis, *supra* note 15.

should be analyzed as such. We urge courts to acknowledge that, in the interest of reducing data insecurity, companies entrusted with the sensitive information of others have a duty to secure data in their systems. We also propose a modified version of the data breach compensation fund proposal recently put forth by Riedy and Hanus.[34]

Data insecurity is an important problem that requires a solution. Advances in cybersecurity are often met with advances in cyber intrusions. Fortunately, as we demonstrate below, the common law is well-suited for recognizing data insecurity as the basis for a legal duty and as the source of injury.

II. DATA BREACHES AND DATA MISUSE

Network security issues impact lives around the world, but the legal field has been scratching its collective head. Data insecurity creates harms that courts are unsure how to address. This Article is most concerned with harms caused by data breaches and data misuse. These phrases are used frequently in the literature, but we find it useful to mark the distinction between the two.

When a data breach occurs, the common factor is a loss of exclusivity for the breached information. A data breach might lead to a variety of outcomes, but the breach exists because information that was supposed to have a limited audience was exposed. Data misuse, on the other hand, exists when there is an unauthorized data use. Identity theft is not caused by a data breach, but rather by a misuse of sensitive data. Data breaches and data misuses thus may occur together or separately. While a data breach might be accidental, data misuse would generally involve a volitional act by someone.

A. Data Breaches

There are three main causes for data breaches: (1) improper disclosure or disposal of sensitive data, (2) loss or theft of hardware containing sensitive data, and (3) computer hacks.[35] Most states have laws governing data breach responses, though these laws often do not require much more than notification of a breach.[36]

Data breaches may be the result of an internal or external threat.[37] Internal incidents can be accidental or on purpose.[38] In 2006, the Board of Education of the City of Chicago inadvertently included home addresses, insurance infor-

34. *See* Reidy & Hanus, *supra* note 28, at 9.

35. Romanosky, Hoffman & Acquisti, *supra* note 30, at 84.

36. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

37. Simpson, *supra* note 3, at 677; *see also* Riedy & Hanus, *supra* note 28, at 15 (noting that hacking by insiders and outsiders accounts for 70% of data breaches); Rowe, *supra* note 1, at 36 (noting that insider threats are a key security concern).

38. *See, e.g.*, Christopher Budd, *Debunking Breach Myths: Who Is Stealing Your Data?*, TRENDMICRO: SIMPLYSECURITY (Oct. 1, 2015), https://blog.trendmicro.com/debunking-breach-myths-who-is-stealing-your-data/.

mation, and social security numbers of 1,750 former employees in a mailing concerning COBRA open enrollment.[39] In late 2017, a hospital in Pequannock, New Jersey experienced a data breach when a former employee stole a hospital hard drive and sold the hard drive online.[40] The hospital hard drive was thought to contain ten years of patient data.[41]

Some lost hardware data breaches with internal causes are accidental. Sometimes, data literally falls off the back of a truck, as in the case of a data breach affecting IBM employees.[42] Recall Total Information Management had contracted with IBM to store and transport data tapes, and then subcontracted part of the transportation to Executive Logistics Services, whose driver then lost the tapes in transit.[43] *In re SAIC* is another recent data breach case that involves data tapes, but in that situation, the tapes were among other items stolen from an employee's car in a public parking lot.[44] In addition to the theft of a GPS system and car stereo, the unfortunate employee also lost copies of the medical records of 4.7 million U.S. military families who were enrolled in TRICARE.[45]

Malicious hacking is often enabled by software defects, with human error as a common indirect cause.[46] When a breach is caused by a malicious outsider, ideally society would be able to hold the actual harm-doer responsible. Yet it is very difficult to identify the source of a cyberattack.[47] As such, when sensitive records are compromised, injured parties may be unable to obtain any kind of redress under a strict regime that only allows for liability for identified attackers. This Article explores other foundations for data breach liability.

There are three primary possible outcomes from a typical data breach for the data subjects: (1) nothing happens and some people just stay nervous forever; (2) some attempted identity theft occurs; and/or (3) the perpetrators post the stolen data online. Sometimes after a data breach, such data dumps are used as a humiliation or intimidation tactic. This practice is sometimes referred to as "organizational doxing."[48] The Ashley Madison hack and subsequent data dump is an example of organizational doxing being used as a tool to punish what the perpetrator views as immoral or unethical behavior.[49] In that situation, the hackers demanded that the adultery-facilitating website be shut down and

39. Cooney v. Chi. Pub. Sch., 943 N.E.2d 23, 27 (Ill. App. Ct. 2010).

40. *Hard Drive Containing Personal Hospital Records Sold Online*, NEWS12 N.J. (Dec. 19, 2017), http://newjersey.news12.com/story/37103529/hard-drive-containing-personal-hospital-records-sold-online.

41. *Id.*

42. Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 115 A.3d 458, 459 (Conn. 2015).

43. *Id.*

44. *In re* Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 19 (D.D.C. 2014).

45. *Id.*

46. Riedy & Hanus, *supra* note 28, at 13.

47. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECH., POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 41 (William A. Owens et al. eds., 2009).

48. Colin J.A. Oldberg, Note, *Organizational Doxing: Disaster on the Doorstep*, 15 COLO. TECH. L.J. 181, 183 (2016).

49. *Id.* at 189.

said they would post member information if their demands were not met, and then the hackers followed through with that threat.[50] Risks to the integrity of data compound data security injuries. In addition to the organization and data subjects losing the exclusivity of their information, it is also very easy for a malicious actor to plant little lies in the data dumps.[51]

1. Impact

Consider a cyberattack resulting in the theft of credit card information. There is a winding path that personal financial information can take after a data theft. Data breaches of electronic payment data create the foundation for a whole shadow industry.[52] Simpson's retelling casts the hacker as the manufacturer that collects the raw data.[53] The hacker sells to wholesalers, wholesalers sell to middlemen who use the data to create cloned credit cards, the middlemen sell the cards to criminal gangs, and the gangs either launder the cards by using them to purchase other gift cards or sell the cards on the street.[54] The purchaser can then use the card until it gets canceled.

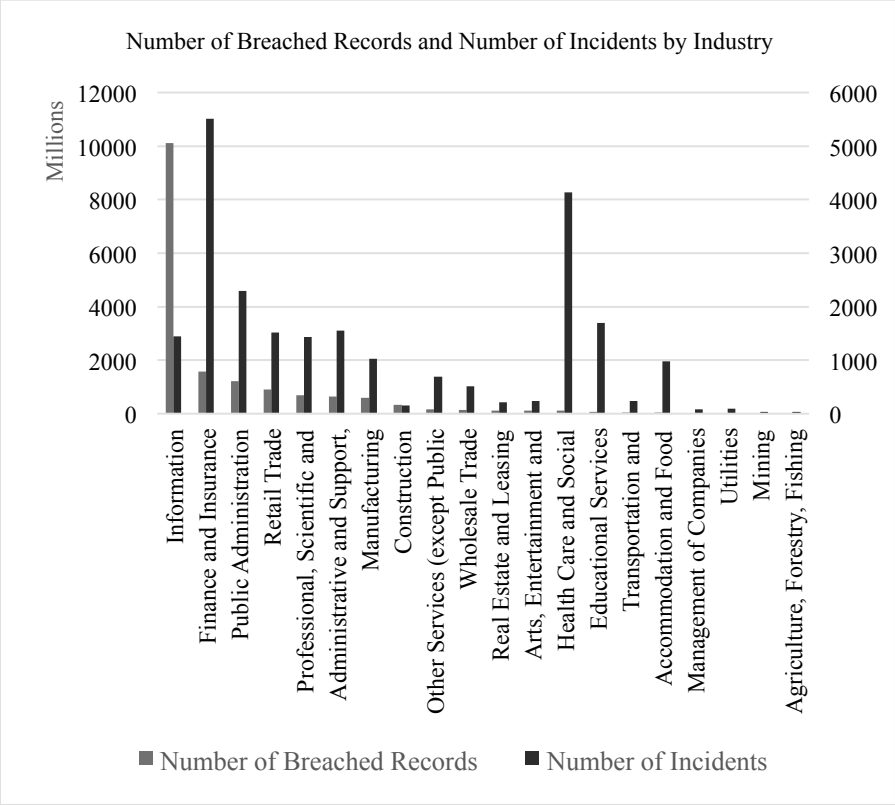
Data breaches are often viewed in terms of their financial impact. The United States currently suffers the highest financial costs of data breaches, with an estimated loss of $225 per record lost.[55] Of that $225 per record, approximately $146 is attributable to the indirect costs of data breaches, which include things like notification costs, the cost of investigations, and loss of customer goodwill.[56] The loss of business alone is credited with an average of $4.13 million in losses for companies in the United States, where the average organizational cost of a data breach is $7.35 million.[57]

Not all industries are affected equally by data breaches.[58] Using raw data obtained from Advisen's records,[59] we have analyzed data breach incidents in the United States by industry, year, number of records breached, and number of incidents. The data was organized into twenty industry categories.[60] Between

50. *Id.* at 188.
51. *Id.* at 191.
52. *See* Simpson, *supra* note 3, at 679–80.
53. *See id.* at 679.
54. *Id.* at 679–80.
55. PONEMON INST., *supra* note 32, at 5.
56. *Id.* at 5–6.
57. *Id.* at 7, 10.
58. Riedy & Hanus, *supra* note 28, at 12.
59. Our research team purchased access to Advisen's data. *Cyber Loss Data*, ADVISEN https://www.advisenltd.com/data/cyber-loss-data/ (last visited Nov. 2, 2018) (data set on file with author). We had some reservations about using data to highlight security incidents because the nature of cybersecurity is mutating so rapidly that relying on findings from any given year to make plans going forward will lead to a constant game of catch-up.
60. *Id.* The twenty industry categories are information, finance and insurance, public administration, retail trade, professional services, administrative and support services, manufacturing, construction, wholesale trade, real estate and leasing, arts and recreation, health care and social assistance, educational services, transportation and warehousing, accommodation and food services, management of companies and enterprises, utilities, mining, other services, and industries related to agriculture, forestry, fishing, and hunting.

2005 and 2014, the information services industry suffered the highest number of breached records at over 10 billion compromised records, while the finance and insurance industries had the highest number of total incidents at 5,512.[61]

FIGURE 1: DATA BREACH INCIDENTS AND RECORDS COMPROMISED, BY INDUSTRY



This figure shows that the Finance and Insurance industry had the highest number of incidents, followed closely by the Healthcare industry. The Information Technology industry, on the other hand, dwarfs all other industry categories for the number of records breached.

The Advisen data also provides a historical context for data breach incidents. The following figures show that between 2005 and 2014, the number of records breached peaked in 2008, but the number of incidents peaked in 2010.

61. *Id.*

FIGURE 2: NUMBER OF BREACHED RECORDS, 2005–2014

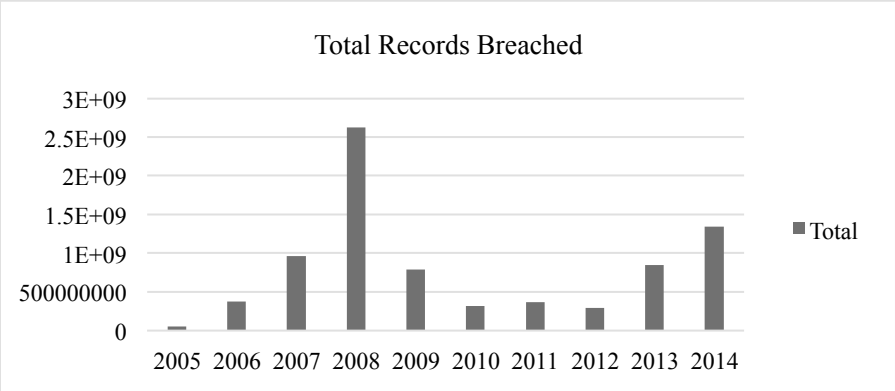
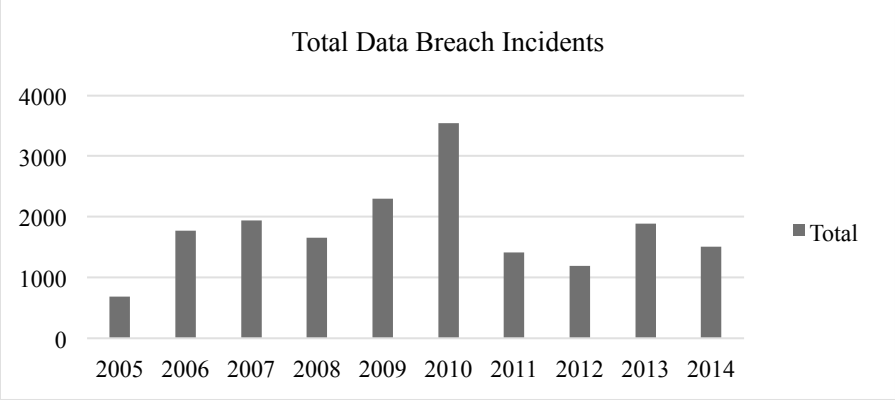


FIGURE 3: NUMBER OF DATA BREACH INCIDENTS, 2005–2014



B. Data Misuse

Consumers routinely enter into agreements about their data, and these agreements often specify how the data recipient might use the data. One type of data misuse occurs when these terms are violated. For the purposes of this Article, we are especially interested in data misuse by the party entrusted with protecting the data. To address the lack of accountability between data traders and data subjects, Ludington proposed the creation of a tort for data misuse.[62]

This is an area where there may be some overlap between tort law and contract law. In the context of social media, a data misuse claim might arise against a person or company who violated an agreement involving someone else's data. That kind of data misuse is related to a breach of contract, but the tools available under contract law might prove inadequate to address data inju-

62. Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 140 (2006).

ries. As we discuss in later sections, data injuries are personal injuries that impact personal autonomy.[63] Because of the nature of these injuries, data misuse that results in data injury would be more appropriately addressed through tort law even when it also involves the violation of a contract.

The social media giant Facebook is at the center of a recent major data misuse controversy involving Cambridge Analytica.[64] It is important to note at the outset that this controversy has potentially serious regulatory consequences for Facebook. In 2011, Facebook entered into a consent decree with the FTC that bars Facebook "from making misrepresentations about the privacy or security of consumers' personal information."[65] A violation of the consent decree could result in fines of up to $40,000 per violation.[66]

In 2010, Facebook made a change in its platform to allow third-party app developers to have more access to Facebook users.[67] In the terms of service for third-party developers, Facebook prohibited third-party app developers from selling user data to others, but these terms proved difficult to enforce.[68] The third-party apps would have to get a user's permission during the installation of the app, but once that permission was granted, they had access to the specified user data.[69] For example, the FourSquare app was used for "checking in" at physical locations, and the user could spend a single click and the app would post the user's location to their Facebook friends.[70] To do this, the app would need access to the user's location, the authority to post on the user's behalf, and access to the user's "friends list" to identify friends who use the app.[71]

By default, a lot of these apps asked for a lot of access, but users had the ability to opt out of some of these requests.[72] Opting out of data collection generally required unchecking boxes during the initial installation of the app.[73] Experts critique the use of opt-out mechanisms because of the bias that people

63. *See infra* Subsection IV.A.3.

64. Chen & Potenza, *supra* note 16.

65. Press Release, Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

66. Natasha Lomas, *Zuckerberg Makes Case for Privacy Regs with Teeth–By Failing to Remember Non-Existent FTC Fine*, TECHCRUNCH (Apr. 11, 2018), https://techcrunch.com/2018/04/11/zuckerberg-makes-case-for-privacy-regs-with-teeth-by-failing-to-remember-non-existent-ftc-fine/.

67. Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

68. *See* Carol Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

69. Meredith, *supra* note 67.

70. *See* Elizabeth Stinson, *Foursquare May Have Grown Up, But the Check-In Still Matters*, WIRED (Aug. 9, 2017), https://www.wired.com/story/foursquare-may-have-grown-up-but-the-check-in-still-matters/.

71. *See Foursquare Labs, Inc. Privacy Policy*, FOURSQUARE, https://foursquare.com/legal/privacy (last updated May 25, 2018).

72. Facebook, *App Privacy with Timeline*, YOUTUBE (Mar. 14, 2012), https://www.youtube.com/watch?v=zkaVXq_HsGk.

73. *Id.*

show towards default settings.[74] Privacy advocates often emphasize the importance of making data collection an opt-in activity.[75]

In 2013, an academic researcher named Aleksandr Kogan created a third-party Facebook app called "This Is Your Digital Life."[76] The app consisted of a personality test, and the default app permissions were extremely broad. 300,000 people installed the app.[77] Some of the people who installed the app gave the app access to not only their friends list, but also their private messages.[78] All told, the 300,000 installations allowed Kogan's app to access the Facebook profile information of 87 million users. Kogan allegedly downloaded all of the data he had access to, and then sold that data to interested parties, including Cambridge Analytica.[79] Armed with detailed records, Cambridge Analytica created psychographic profiles of users, and those profiles were allegedly used to develop products to promote fake news stories and propaganda to influence elections and support specific political campaigns.[80]

In summary, for several years, Facebook allowed third-party app developers to request broad access to user data, and many apps requested more information than was strictly necessary for the app's purpose.[81] Kogan took advantage of this design with "This Is Your Digital Life" and harvested information on 300,000 app installers and about 87 million of their closest friends.[82] Kogan sold the data to Cambridge Analytica, which then allegedly used the data to help politicians get elected.[83] Any claim involving data misuse thus would probably focus on Kogan's intentional violation of the terms of his agreement with Facebook, and also on Facebook's failure to adequately police the use of data on its platform.

Mark Zuckerberg, the founder and CEO of Facebook, was immediately under intense scrutiny by the media and the government. During hearings before Congress, Zuckerberg noted several times that this chain of events would not be possible on Facebook's current platform because in 2014, Facebook significantly curbed the potential access of third-party apps.[84] Zuckerberg also told the Senate that in 2015, when Facebook learned that Kogan had violated the terms of his agreement with the company, Facebook demanded that both Kogan

74. *See* Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 66–67 (2014).

75. *See* Paul M. Schwartz, *Property, Privacy, And Personal Data*, 117 HARV. L. REV. 2055, 2100 (2004).

76. Meredith, *supra* note 67.

77. *Id.*

78. Issie Lapowsky, *Cambridge Analytica Could Have Also Accessed Private Facebook Messages*, WIRED (Apr. 10, 2018), https://www.wired.com/story/cambridge-analytica-private-facebook-messages/.

79. *Id.*; Meredith, *supra* note 67.

80. *See* Meredith, *supra* note 67.

81. *See id.*

82. *Id.*; Lapowsky, *supra* note 78.

83. *See* Meredith, *supra* note 67.

84. Bloomberg Gov't, *Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.a39f8b2eb57e.

and Cambridge Analytica delete the misappropriated data from their systems.[85] When asked if the company had disclosed this incident to the Federal Trade Commission pursuant to the consent decree of 2011, Zuckerberg told the Senate that Facebook had not notified the FTC because they considered it a "closed" issue.[86]

The Facebook controversy is particularly compelling because advertising is their business model, but most users arguably do not realize the extent of Facebook's knowledge about their online lives. Even users who are fully aware of the company's business practices are not consenting to be targeted by everyone using the same information.

C. Addressing Data Security Issues

Business leaders are increasingly recognizing the importance of cybersecurity. In PWC's Annual Global CEO Survey for 2018, 40% of CEOs expressed that they were "extremely concerned" about cybersecurity, up from 24% in the 2017 survey.[87]

There are three major legal avenues for addressing data security issues: (1) legislation, (2) administrative agency action, and (3) litigation. In the absence of a clear legal framework, or perhaps to avoid the creation of a clear legal framework, some industries self-regulate. The Payment Card Industry Data Security Standard ("PCI DSS") is an example of self-regulation.[88]

As the following subsections show, legal commentary about how to address data insecurity risks varies, though most suggestions rely on either judges or some other form of government action. Some call for comprehensive federal legislation, others think the FTC or another agency should regulate data breach concerns, and a third group advocates for the evolution of tort law. Riedy and Hanus suggest creating a data victims' compensation fund instead of relying on litigation.[89] Such a fund might limit payouts to compensable "out-of-pocket losses directly caused by the breach."[90] Some have also suggested malpractice liability for computer security professionals.[91] This Article takes a comprehensive approach to addressing data injuries and significantly contributes to the limited, existing literature that looks for common law solutions for data insecurity injuries.

85. *Id.*

86. PBS NewsHour, *WATCH LIVE: Facebook CEO Mark Zuckerberg Testifies before Senate on User Data*, YOUTUBE (Apr. 10, 2018), https://www.youtube.com/watch?v=qAZiDRonYZI.

87. *Threats: What Keeps CEOs Up at Night Differs By Region*, PWC, https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx/business-threats.html (last visited Nov. 2, 2018).

88. *See* Callie E. Waers, *More Than An Upgrade: Payment Card Industry Data Security Standards*, 58 DRI 49, 49–51 (Feb. 2016) (discussing Genesco, Inc. v. Visa USA, Inc., which concerned PCI DSS noncompliance).

89. Riedy & Hanus, *supra* note 28, at 45.

90. *Id.* at 48.

91. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1590.

1. Cybercrime and Privacy Statutes

For over thirty years, litigants, academics, and policymakers have pursued shifting theories of liability for cyber intrusions. The most obvious theory of liability is to hold the most culpable actors liable—the malicious intruders and data thieves.

The Computer Fraud and Abuse Act ("CFAA") is the federal criminal statute that is most applicable to cybersecurity events like data breaches.[92] Section 1030(a)(2) of the CFAA broadly prohibits parties from accessing a protected computer and obtaining information when the party does not have authorization to do so, or exceeds their authorization in doing so.[93] Section 1030(a)(5)(A) prohibits harmful transmissions,[94] and Section 1030(a)(6) prohibits trafficking in passwords.[95]

Each state also has its own cybercrime laws. Most states include CFAA-like language about authorization and access offenses, including unlawful acts aimed at obtaining data. In addition, eight states also prohibit receiving data that was obtained unlawfully.[96] Many state laws emphasize tools. Fourteen states carve out an explicit prohibition on keystroke loggers.[97] Five states prohibit the use of encryption in the course of committing another criminal offense.[98] Four states use their cybercrime laws to call out botnets.[99]

Unfortunately, cybercriminals have evolved to address every new challenge.[100] Further, accurate attribution of a cyberattack has always been very difficult. Out of necessity, theories of liability began to shift. One example of this

92. 18 U.S.C. § 1030 (2018).

93. *Id.* § 1030(a)(2) ("Whoever—intentionally accesses a computer without authorization or exceeds authorized access . . . shall be punished as provided in subsection (c) of this section.").

94. *Id.* § 1030(a)(5)(A) ("[K]nowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . .").

95. *Id.* § 1030(a)(6) ("[K]nowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization . . . .").

96. *See* CONN. GEN. STAT. § 53a-251(e)(3) (2018); DEL. CODE ANN. tit. 11, § 935(3) (2018); KY. REV. STAT. ANN. § 434.855 (West 2018); MO. REV. STAT. § 569.095(1)(6) (2018); N.H. REV. STAT. ANN. § 638:17(IV)(c) (2018); N.Y. PENAL LAW § 156.35 (McKinney 2018); TENN. CODE ANN. § 39-14-602(c) (2018); W. VA. CODE ANN. § 61-3C-9 (LexisNexis 2018).

97. *See* ALASKA STAT. § 11.46.740(a)(2) (2018); ARIZ. REV. STAT. ANN. § 18-502(A)(2)(a) (2018); ARK. CODE ANN. § 4-111-103(a)(2)(A) (2018); CAL. BUS. & PROF. CODE § 22947.2(b)(1) (West 2018); GA. CODE ANN. § 16-9-152(a)(2)(A) (2018); IOWA CODE § 715.4(2) (2018); LA. STAT. ANN. § 51:2008(2)(a) (2018); N.H. REV. STAT. ANN. § 359-H:2(III) (2018); 73 PA. STAT. AND CONST. STATE. ANN. § 2330.3 (West 2018); 11 R.I. GEN. LAWS § 11-52.2-2(2)(a) (2018); TEX. BUS. & COM. CODE ANN. § 324.051(1)(A) (West 2018); UTAH CODE ANN. § 13-40-301(2)(a) (West 2018); VA. CODE ANN. § 18.2-152.4(A)(8) (2018); WASH. REV. CODE § 19.270.020(2) (2018).

98. *See* ARK. CODE ANN. § 5-41-204(a)(1) (2018); 720 ILL. COMP. STAT. 5/17-52.5(b)(1) (2018); MINN. STAT. § 609.8912 (2017); NEV. REV. STAT. § 205.486(1) (2017); VA. CODE ANN. § 18.2-152.15 (2018).

99. *See* LA. STAT. ANN. § 51:2009(1)(c) (2018); N.H. REV. STAT. ANN. § 359-H:2(I)(c) (2018); TEX. BUS. & COM. CODE ANN. § 324.055(b) (West 2018); WASH. REV. CODE § 19.270.020(8) (2018).

100. *See* Riedy & Hanus, *supra* note 28, at 21–22; Michael L. Rustad & Thomas H. Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOK. L. REV. 1, 101–02 (2002) [hereinafter Rustad & Koenig, *Tort Monster*] (recommending changes in tort law to account for new cybercrimes).

shift is the fact that eight states prohibit the receipt of data obtained unlawfully.[101] Additionally, seven states prohibit the act of trafficking in software that falsifies email transmission information.[102]

If the cybercriminals cannot be caught, the legal system should still support strengthening the defenses, because good network security is in the public interest. That is the basic rationale for finding less culpable actors liable for cybersecurity harms, and also is a philosophical foundation for a duty to secure data. In some situations, state cybercrime laws have adapted to find liability. Email spoofing is commonly associated with phishing attacks.[103] By criminalizing the act of trafficking in software that enables email spoofing, states are looking upstream to the product's supplier.[104] By criminalizing the receipt of unlawfully obtained information, legislators are looking downstream of the data thief to the potentially more identifiable information recipients.

The CFAA, however, has remained fairly static. The last time the CFAA was amended was September 2008.[105] Courts briefly flirted with an interpretation of the CFAA that would impose transmission liability on software manufacturers whose products contained serious bugs.[106] That interpretation was foreclosed with the passage of the USA PATRIOT Act, which among other things amended Section 1030(g) to add one sentence to the end: "No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."[107] In eliminating upstream CFAA liability for software manufacturers, Congress implicitly affirmed that the CFAA remains primarily focused on liability for the most culpable party.

Other federal laws, however, support shifting liability towards the party most able to protect sensitive data from disclosure. The Health Insurance Portability and Accountability Act ("HIPAA"), for example, has strict privacy and security rules. Covered entities are required to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [protected health information]."[108]

101. *See supra* note 96 and accompanying text.

102. *See* CONN. GEN. STAT. § 53-451(c) (2018); 720 ILL. COMP. STAT. 5/17-51(a-5) (2018); LA. STAT. ANN. § 14:73.6(B)(1) (2018); NEV. REV. STAT. § 205.492(3) (2017); 18 PA. STAT. AND CONS. STAT. ANN. § 7661(a)(2) (West 2018); 11 R.I. GEN. LAWS § 11-52-4.1(a)(8) (2018); VA. CODE. ANN. § 18.2-152.3:1(A)(2) (2018).

103. *See* Simpson, *supra* note 3, at 678, 678 n.62.

104. Most of the laws concerning falsification software are found within anti-spam sections. The upstream focus on providers of the software can reduce both spam and phishing-based email spoofing.

105. Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, sec. 203–08, § 1030, 122 Stat. 3560, 3561–64 (2008).

106. Shaw v. Toshiba America Info. Sys., Inc., 91 F. Supp. 2d 926 (E.D. Tex. 1999) (denying defendants' motions for summary judgment where plaintiffs alleged defendants distributed faulty software in violation of the CFAA).

107. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 384 (2001) (codified as amended at 18 U.S.C. § 1030(g) (2001)).

108. 45 C.F.R. § 164.306(a)(2) (2017).

Federal privacy laws in the United States are largely sector-specific, and generally emphasize the protection of "personally identifiable information," or a reasonable variation thereof. We've already mentioned HIPAA, which applies to healthcare providers. The Privacy Act of 1974 applies to federal agencies. The Privacy Act of 1974 requires agencies to have technical safeguards in place "to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[109]

There are also federal privacy laws governing the financial sector. The Gramm-Leach-Bliley Act ("GLBA") requires financial institutions to adopt safeguards to protect customer information against "any anticipated threats or hazards to the security or integrity of such records."[110] The GLBA further requires covered entities to protect against access or use of customer records "which could result in substantial harm or inconvenience to any customer."[111] There are several other sector-specific federal privacy laws, but for our purposes, the security requirements of HIPAA, the Privacy Act, and the GLBA are especially relevant.

The trend of legislative solutions imposing liability on third parties is consistent with similar themes in tort law. For example, the last clear chance doctrine arises in the context of contributory negligence. Even if the plaintiff's injury was partially due to their own negligence, if the defendant had the last clear chance to prevent the injury, liability would attach to the defendant.[112] In the event of a cyberattack by a third party, HIPAA, the Privacy Act, and GLBA all impose liability under federal law on the party with the last clear chance of avoiding information theft. FTC enforcement actions against data breach targets are intended to have a similar effect. By increasing the incentives to secure data, either through carrots or sticks, government actions can contribute to a stronger cybersecurity environment.

There are frequent calls for Congress to enact comprehensive federal data privacy legislation.[113] Such legislation could create a private cause of action to reduce uncertainty about things like duty and injuries.[114] Skeptics, though, question the political feasibility of passing a data privacy statute in a Congress that often acts for the benefit of businesses.[115] The recent hearings in the House

109. Privacy Act of 1974, 5 U.S.C. § 552a(e)(10) (2018).

110. Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b)(2) (2018).

111. *Id.* § 6801(b)(3).

112. *See generally* Malcolm M. MacIntyre, *The Rationale of Last Clear Chance*, 53 HARV. L. REV. 1225 (1940).

113. Patricia Cave, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. Rev. 765, 789 (2013); Romanosky, Hoffman & Acquisti, *supra* note 30, at 100; Evan M. Wooten, *The State of Data Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CAL. 229, 239 (2015).

114. Cave, *supra* note 113, at 787; Simpson, *supra* note 3, at 691-92; Wooten, *supra* note 113, at 239.

115. Martecchini, *supra* note 20, at 1494–95.

and Senate about Facebook's data practices underscore the tension present in this area.[116]

The United States and the European Union have very different approaches to informational privacy. In the United States, the constitutional right of privacy is enforceable against infringement by the government and state actors.[117] Rights of privacy that can be enforced against private citizens are either a creature of tort law or the result of statutes covering specific types of information. The privacy law regime of the United States is often described as a patchwork of fixes, a dynamic that is especially obvious in the example of the Video Privacy Protection Act ("VPPA").[118] The VPPA's enactment was inspired largely by a controversy surrounding the nomination of Robert Bork to the Supreme Court when the media obtained information about the Bork family's video rental history.[119] This patchwork approach to privacy regulation is why Netflix viewing habits may be more protected than a Google search history.

EU privacy law, on the other hand, restricts privacy infringements by both the public and private sectors.[120] EU law also adopts a very broad definition of personal data as "any information relating to an identified or identifiable natural person."[121] Simpson attributes European vigilance on data privacy as stemming from the continent's recent experiences with surveillance in totalitarian governments.[122]

Some scholars have suggested that the United States should adopt laws that are more protective of data, like those of the European Union.[123] In May of 2018, the new General Data Protection Regulation ("GDPR") for the European Union went into effect, replacing the 1995 directive.[124] The GDPR drops the familiar language of "personal data," instead using a broader category that includes things like IP addresses and biometric data.[125] The GDPR also requires data holders to obtain consent prior to engaging in the processing of data,

116. Seth Fiegerman, *Congress Grilled Facebook's Mark Zuckerberg for Nearly 10 Hours. What's Next?*, CNN TECH (Apr. 12, 2018, 3:30 PM), http://money.cnn.com/2018/04/12/technology/facebook-hearing-what-next/index.html.

117. Michael L. Rustad & Thomas H. Koenig, *Negligent Entrustment Liability for Outsourced Data*, 10 J. INTERNET L. 3, 4–5 (2007) [hereinafter Rustad & Koenig, *Outsourced*].

118. Ludington, *supra* note 62, at 152–53.

119. *Id.*

120. *Data Protection and Online Privacy*, EUROPEAN UNION: YOUR EUROPE, https://europa.eu/your europe/citizens/consumers/internet-telecoms/data-protection-privacy/index_en.htm (last updated June 7, 2018).

121. Regulation 2016/679, art. 4, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 33; Simpson, *supra* note 3, at 699–700.

122. Simpson, *supra* note 3, at 702.

123. *See, e.g.*, Cave, *supra* note 113; Ludington, *supra* note 62, at 189 (noting that sweeping federal legislation would be preferable to expanding tort law); Rustad & Koenig, *Outsourced*, *supra* note 117; Simpson, *supra* note 3.

124. Council Regulation 2016/679, art. 99, 2016 O.J. (L 119) 1, 2 (EU).

125. *Compare id.* at art. 9, 1 (including biometric data in the operative portion of the statute), *with* Council Directive 95/46, art. 8, 1995 O.J. (L 281) 1 (EC) (limiting the prohibition on the processing of personal data to "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life").

where processing is broadly defined as any operations performed on personal data.[126] Consent under the GDPR must be "freely given, specific, informed and unambiguous."[127]

2. Administrative Agencies

Administrative agencies are empowered by Congress to carry out specific categories of duties. The Department of Homeland Security ("DHS") is the most active agency when it comes to cybersecurity,[128] but other agencies also address how regulated entities should handle data insecurity issues. The Federal Trade Commission ("FTC") is the main administrative agency that might initiate an action against a company after a security breach.[129] The FTC's authority is based on Section 5 of the FTC Act, which gives the agency the authority to address unfair or deceptive business practices.[130] The Securities and Exchange Commission ("SEC") has issued guidance documents about cybersecurity.[131] The CFPB is another possible agency that could get involved because of its emphasis on consumer protection, but at the time of this writing, the current head of the CFPB seemingly does not think that data security is within the CFPB's purview.[132]

The National Institute of Standards and Technology ("NIST") is a non-regulatory agency within the Department of Commerce. NIST's focus is on supporting innovation, and to this end, NIST was entrusted with crafting a voluntary set of cybersecurity standards, the Cybersecurity Framework ("CSF").[133] The CSF provides information about best practices in the cybersecurity realm.[134] Though the CSF was originally conceived of as a way to address uniquely vulnerable critical infrastructure, it also centralizes information that can be valuable to other industries. This Article proposes that courts establish a clear duty to secure data. If such a duty is recognized, the CSF and similar resources could be very valuable when courts are evaluating whether the defendant breached that duty.

126. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 1(a) (EU).

127. *Id.* at art. 4(11).

128. *Cybersecurity*, DHS.GOV, https://www.dhs.gov/topic/cybersecurity (last visited Nov. 2, 2018).

129. Cave, *supra* note 113, at 789–790; Robert L. Rabin, *Perspectives on Privacy, Data Security and Tort Law*, 66 DEPAUL L. REV. 313, 336–37 (2017) [hereinafter Rabin, *Data*]; Simpson, *supra* note 3, at 705; Wooten, *supra* note 113, at 242.

130. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015); Rabin, *Data*, *supra* note 129, at 336 (suggesting that the Wyndham decision shows that the FTC could potentially address data security issues in the law without an expansion of tort law).

131. Public Statement by Jay Clayton, SEC Chairman, Statement on Cybersecurity Interpretive Guidance (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21; Roberta D. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 TORT. TRIAL & INS. PRAC. L.J. 529, 531 (2014).

132. Rucker, *supra* note 13.

133. Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,740–41 (Feb. 12, 2013) [hereinafter Exec. Order]; National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, (Apr. 16, 2018) [hereinafter NIST], https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

134. NIST, *supra* note 133.

3. Civil Suits

Historically, courts have occasionally participated in social changes by modernizing the law when legislatures have been slow to respond to emerging trends.[135] Ludington notes that plaintiffs used common law torts to combat sexual harassment until legislation caught up via Title VII of the Civil Rights Act of 1964.[136] In his book, *The Cost of Accidents*, Guido Calabresi argues that civil litigation can be used to control the costs of accidents and shift the burden to the party best able to prevent the accident.[137] Rustad and Koenig point out that tort law has also historically been used to address abuses of power by corporations.[138]

The Supreme Court said in 1884 that the "flexibility and capacity for growth and adaptation is the peculiar boast and excellence of the common law."[139] Courts and scholars have considered various options for tort evolution to better address network-based injuries. In *Intel Corp. v. Hamidi*, Internet-enabled injuries from a high volume of e-mail traffic were analyzed under a trespass to chattels theory.[140] Ludington advocates for tort liability for the misuse of personal data, reasoning that such liability would create incentives to handle data responsibly.[141] There are a lot of costs associated with cybersecurity incidents, many of which seem to fall on third parties.[142]

One possible approach is to expand privacy torts to better bring data insecurity injuries into the fold.[143] Gasser argues that the "current digital privacy crisis" should be addressed by "[r]eimagining the relationship between technology and privacy law in the digital age."[144] This is what many scholars try to do when analyzing modern privacy issues. Richards and Solove suggest making the breach of confidence tort more robust in American courts.[145] Another option is to require data holders to adhere to Fair Information Practices

135. Ludington, *supra* note 62, at 171; Rustad & Koenig, *Tort Monster*, *supra* note 100, at 6.

136. Ludington, *supra* note 62, at 188.

137. GUIDO CALABRESI, THE COST OF ACCIDENTS 244–45 (1970); Erica Goldberg, *Emotional Duties*, 47 CONN. L. REV. 809, 851 (2015); Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1598.

138. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 103; *see also* Goldberg, *supra* note 137, at 850 (discussing tort theory in the law and economics movement).

139. Hurtado v. California, 110 U.S. 516, 530 (1884).

140. 71 P.3d 296, 311 (Cal. 2003) ("We therefore decline to create an exception, covering Hamidi's unwanted electronic messages to Intel employees, to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury . . . ."); Rustad & Koenig, *Tort Monster*, *supra* note 100, at 94.

141. Ludington, *supra* note 62, at 146; *see also* Vincent R. Johnson, *Data Security and Tort Liability*, 11 NO. 7 J. INTERNET L. 22, 30 (2008) ("Tort law offers an appropriate legal regime for allocating the risks and spreading the costs of database intrusion-related losses.").

142. Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27, 31–32 (2007); Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1556.

143. Ludington, *supra* note 62, at 140; Oldberg, *supra* note 48, at 204 (2016).

144. Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61, 69 (2016).

145. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1922 (2010).

("FIPs").[146] Ludington also suggests that lax security practices could potentially amount to a constructive publication that will meet the publicity requirement for the public disclosure tort.[147] In fact, this is not too far from the interpretation that the Fourth Circuit adopted with regard to publication-related terms in insurance policies that might cover data breaches.[148]

Liability issues for lost hardware data breaches and purely electronic data breaches are generally treated similarly by courts, but this may be a mistake. When physical storage is stolen, the motive can be based on the value of the equipment or on the value of the information.[149] When digital data is compromised directly, there is not a question as to whether the data or the equipment was the target, because no physical equipment is implicated. As such, a data insecurity injury is likely to be more serious in purely electronic data breaches because there is less ambiguity about the thief's intentions.

In the United States, a country with a reputation for being litigious, data breach lawsuits are far from predictable. An empirical study found that breached entities are more likely to be sued when the breach affected more people or when individuals have already suffered financial harm from the breach.[150] Entities that provided free credit monitoring to victims have historically been sued at lower rates.[151] Offering free credit monitoring does not seem to have a significant downside in litigation, since generally courts have not been receptive to arguments that offering free credit monitoring is an admission of guilt.[152]

In Romanosky's data set, 76% of the lawsuits were class actions.[153] Once a data breach lawsuit is brought, Romanosky's calculations suggest that there is approximately a 50/50 chance that the lawsuit will end in a settlement.[154] Many of the remaining lawsuits still do not make it out of the pretrial stage.

The same study found no fewer than eighty-six unique causes of action in data breach cases.[155] Some of the common claims were founded in state unfair business practice laws, the federal Fair Credit Reporting Act, breach of contract, and negligence.[156]

Much of this Article focuses on a negligence framework, but the application of other causes of action merits note. For example, in data breach cases against LinkedIn and Sony Interactive Entertainment (formerly Sony Computer Entertainment), courts acknowledged the validity of claims under California's

146. Ludington, *supra* note 62, at 173–74. The four FIPs that Ludington cites are notice, choice, access, and security. *Id.* at 173.

147. *Id.* at 164.

148. Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC, 644 F. App'x 245, 247 (4th Cir. 2016).

149. Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017).

150. Romanosky, Hoffman & Acquisti, *supra* note 30, at 74.

151. *Id.*

152. *E.g.*, Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017).

153. Romanosky, Hoffman & Acquisti, *supra* note 30, at 83.

154. *Id.* at 94.

155. *Id.* at 100.

156. *Id.* at 101; Solove & Citron, *supra* note 27, at 11.

unfair business practice laws where the defendants failed to adequately secure customer information.[157] In litigation over a breach affecting TJ Maxx customers, card-issuing banks were blocked from bringing a breach of contract claim unless the banks could establish that they were third-party beneficiaries for the contract between TJ Maxx and its payment processors.[158]

A cynic might look at the high number of causes of action and conclude that attorneys are just throwing claims at the wall to see which ones stick. On the other hand, the variety of claims may indicate that courts and practitioners are struggling to recognize obligations and harms that clearly should be recognized but that don't easily fit into the mold of current legal doctrine. Ultimately, the current state of data breach litigation is due to the lack of a solid legal and ideological foundation for addressing data insecurity injuries. This gap contributes to a lack of trust that further strains relationships between individuals and the companies entrusted with their data.

Data insecurity claims have many barriers in litigation.[159] Rabin criticizes the current legal regime for data breaches because it leaves victims uncompensated, fails to create incentives to improve security, and perpetuates uncertainty about liability.[160] Privacy torts are often inadequate for addressing data insecurity injuries.[161] Negligence claims often fail because of a lack of physical harm.[162] Many data breach lawsuits do not even reach the merits stage because they are dismissed as lacking the concrete and particularized injury required for Article III standing.[163]

A variety of solutions have been suggested. Rabin notes that appropriation of identity claims are more likely to survive a motion to dismiss, but that the contours of the tort often require plaintiffs to show some sort of profit from their personal data.[164] While there is a shadowy industry around the theft and use of credit card numbers, it would be difficult to tie a particular breach to a particular fraudulent incident.

Some scholars suggest strict liability and analogies to products liability.[165] Rustad and Koenig proposed that software manufacturers be held liable under tort law based on negligent enablement of cybercrime.[166] They reasoned that a negligence framework would be preferable to a strict liability approach because

157. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 1013–14 (S.D. Cal. 2014); *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1092–95 (N.D. Cal. 2013); *see also* Wooten, *supra* note 113, at 243–44.

158. *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 499 (1st Cir. 2009).

159. Johnson, *supra* note 141, at 29.

160. Rabin, *Data*, *supra* note 129, at 323.

161. *Id.* at 324–26.

162. Cave, *supra* note 113, at 778.

163. Pinson, *supra* note 142, at 48.

164. Rabin, *Data*, *supra* note 129, at 328.

165. *See* Ludington, *supra* note 62, at 171; Oldberg, *supra* note 48, at 199. Product liability law itself, though, may not be a good fit. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 243 (2007); Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1580.

166. *See* Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1575.

under a negligence theory, a customer's unreasonable security practices could reduce the manufacturer's liability.[167] In a subsequent article, Rustad and Koenig suggested negligent enablement liability for data holders who outsource data-related services.[168]

D. Negligence Framework

We utilize a negligence framework for data injuries. While there may be some bad actor driving the harm, those bad actors are often not caught, and most compromised data holders do not have the requisite intent for an intentional tort claim.[169] Negligence is a fact-intensive inquiry that many feel is best suited for a jury, so summary judgment motions are rarely granted in negligence cases.[170] If data breach litigation adopts a negligence basis, that may mean that trials last longer or settlement rates increase. Ultimately, it may be that negligence is not an appropriate framework, but it is nevertheless useful for analytical purposes.

The negligence framework provided a flexible model of liability during the massive social upheaval of the Industrial Age.[171] McDonald notes that "the inventions and innovations of the Industrial Revolution . . . had a marvelous, unprecedented capacity for smashing the human body."[172] The attractive nuisance doctrine of tort law developed in this time period, allowing property owners to be held liable for injuries to children caused by dangerous things on the property that children used while playing.[173] The versatility of negligence law to address new challenges is the primary reason that we view data insecurity injuries through the lens of negligence.

A negligence analysis asks four main questions: (1) Did the defendant owe a duty to the plaintiff? (2) Did the defendant breach that duty? (3) Did the plaintiff suffer an injury? (4) Was the breach of duty the cause of plaintiff's injury?[174] This Article is primarily interested in addressing the first and third questions. We use legal precedent and reasoning, interdisciplinary insight, and data from reported cybersecurity events to argue that the storage of the sensitive personal data of others imposes a duty to secure that data, and that the data insecurity that results from a breach of this duty is an injury to autonomy. Concluding that data holders have a duty to secure sensitive information is a natural

167. *Id.* at 1561.

168. Rustad & Koenig, *Outsourced*, *supra* note 117, at 3–4.

169. *See* Rabin, *Data*, *supra* note 129, at 330 (noting that as an intentional tort, trespass to chattels is unlikely to help individuals hold companies liable for data breach harms).

170. Cara McDonald, *Torts Law: Blurred Elements: The Nebulous Nature of Foreseeability, the Confounding Quality of Misfeasance, and the Minnesota Supreme Court's Decision*—Doe 169 v. Brandon, 41 WM. MITCHELL L. REV. 365, 395 (2015).

171. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 25–26.

172. McDonald, *supra* note 170, at 370 (internal quotations omitted) (citing LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 350 (3d ed. 2005)).

173. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 33 (giving the example of railroad turntables).

174. McDonald, *supra* note 170, at 369; Rustad & Koenig, *Tort Monster*, *supra* note 100, at 44.

outgrowth of the shifting liability regimes for data-based injuries discussed in Subsection II.A.1.

We should briefly address the causation element of negligence, with the caveat that this element will likely be very fact intensive. Causation is also tricky to observe. Litigants might sometimes appeal to the doctrine of *res ipsa loquitur* to stablish causation for their injury.[175] In the case of a data breach, for instance, it is tempting to conclude that the existence of a breach implies that the data collector had failed to take all of the proper precautions. Because of the rapid evolution of cyberattack methods, a *res ipsa* theory of cybersecurity liability would likely be inadvisable, but this issue is outside the scope of this Article.

Another complication of causation is the presence of intervening criminal behavior in cases involving third-party hackers.[176] In *Stollenwerk v. Tri-West Health Care Alliance*, the Ninth Circuit noted in dicta that under governing Arizona law, "the fact that the identity fraud incidents were committed by third parties does not preclude a finding of proximate cause."[177]

If an action by a third party does not eliminate negligence liability, then that still leaves the problem of connecting the specific data breach with a specific incident of identity theft. If a person's credit card number is stolen and fraudulent charges are made, they will need to at least establish some evidence that the injury was caused by this specific breach.[178]

In a negligence framework, the reasonable foreseeability of a particular outcome factors into the analysis of proximate cause. Foreseeability is also closely tied to duty in negligence law. Foreseeability is a fluid concept that changes with time and technology. In the context of trade secrets, Rowe asserts that the risk of computer-enabled trade secret misappropriation is foreseeable for trade secret owners, and thus courts should examine the reasonableness of a plaintiff's cybersecurity practices.[179] Rustad and Koenig argue, "In a networked world, it is reasonably foreseeable that computer hackers or cybercriminals will discover and exploit known vulnerabilities in operating systems."[180]

Foreseeability has implications for creators and users of insecure software. Software creators, however, often reduce or eliminate their potential liability through clickwrap licenses that users must agree to before they can use the product.[181] That leaves the users of insecure software with the responsibility of preventing foreseeable harm to the data they protect.

175. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1599–1600.

176. Oldberg, *supra* note 48, at 201 (raising and dismissing the concern in favor of a strict liability theory).

177. 254 Fed. App'x. 664, 668 n.2 (9th Cir. 2007).

178. *Id.* at 667 (reversing summary judgment on negligence claim because plaintiff "produced evidence from which a jury could infer a causal relationship between the theft of the hard drives and the incidents of identity fraud . . ."); Riedy & Hanus, *supra* note 28, at 31.

179. Rowe, *supra* note 1, at 26.

180. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1570.

181. *Id.* at 1565.

Some of the major causation issues may be avoided if courts recognize enabling torts. In the 1990s, when lawsuits were being brought against gun manufacturers and tobacco companies, Rabin explored the concept of enabling torts.[182] An enabling tort would be an appropriate cause of action when the defendant negligently created an environment where it becomes more likely that someone else will cause an injury.[183] Rabin's proposal for enabling torts is based in part on the negligent entrustment tort, which might apply in a situation where a car owner allows an intoxicated or unlicensed driver to borrow their car, and that driver subsequently injures a pedestrian.[184]

In some situations, there might be liability for a defendant who acts negligently and then a third party takes advantage of the opening and acts maliciously. Sticking with car examples, Rabin imagines a key left in a car's ignition overnight, setting the stage for grand theft auto.[185] If the thief injures someone while driving the stolen car, should the car's owner be held liable for making the theft so easy?

A car with keys in the ignition will not harm a pedestrian but for the ensuing reckless driving of an opportunistic car thief. An analysis based on the owner's liability, therefore, is predicated upon establishing that a car with keys in the ignition is too tempting a target. This leads to Rabin's theory of an enabling tort, which could impose liability on the person who created the tempting condition.

In a way, the concept of enabling torts can be viewed as an expansion of the idea of attractive nuisance, except instead of hazardous objects attracting children, this is about tempting conditions attracting criminals. Yet, this may undermine the general assumption in the legal system that citizens are and want to be law-abiding.[186] Oliver Wendell Holmes said that "[t]he principle seems to be pretty well established, in this country at least, that everyone has a right to rely upon his fellow-men acting lawfully, and, therefore, is not answerable for himself acting upon the assumption that they will do so, however improbable it may be."[187] Holmes, it would seem, would not be in favor of finding a careless (carless) person liable for injuries caused by a car thief.

The 1921 case of *Hines v. Garrett* is another example of negligence followed by a crime. In *Hines*, an eighteen-year-old girl was riding a train late at night and the driver missed her stop.[188] There was some dispute about whether the conductor pressured her to get off the train almost three-quarters of a mile after her intended stop or if she chose to get off the train of her own free will.[189] The plaintiff was sexually assaulted twice during her walk back to her intended

182. *See generally* Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435 (2000) [hereinafter Rabin, *Enabling Torts*].

183. Rabin, *Data*, *supra* note 129, at 332.

184. Rabin, *Enabling Torts*, *supra* note 182, at 438.

185. *Id.* at 440.

186. Oliver Wendell Holmes, *Privilege, Malice and Intent*, 8 HARV. L. REV. 1, 10 (1894).

187. *Id.*

188. Hines v. Garrett, 108 S.E. 690, 691 (Va. 1921).

189. *Id.* at 692–93.

station and sued the railroad company. The court, while noting the importance of the dispute over the conductor's negligence, concluded that if the conductor had been negligent, the railroad company could be held responsible for the plaintiff's injuries. In other words, liability could attach because the conductor's negligence put the plaintiff into the dangerous situation. This conclusion is further supported by the high duty of care that common carriers like railroads owe to their passengers.[190]

As the above examples illustrate, there are many possible circumstances where causation will be controversial when addressing data breach harms. Causation analysis, though, will likely mirror similar analysis in other negligence cases. Likewise, whether a duty is breached will be based on the same principles as other breach of duty analyses in negligence case law. The nature of digital injuries, however, makes it trickier to directly apply the same principles to evaluating whether a duty exists and whether the plaintiff has suffered a cognizable injury.

III. DUTY

A central part of our analysis in this Article focuses on the legal duty to secure data. There can be no civil liability if the defendant does not owe a duty to the plaintiff. Arguments about the legal duty for negligence often have heavy political implications.[191] Potential defendants typically have more resources than potential plaintiffs, and those resources are frequently more devoted to avoiding than accepting liability. Plaintiffs traditionally face an uphill climb.

Ever since the landmark case of *Palsgraf v. Long Island Railroad Co.*, the presence of a duty has been connected to foreseeability.[192] *Palsgraf* concerned a common mass transit scenario of a passenger rushing to avoid missing a train.[193] In what we assume was a dramatic fashion, the latecomer ran and jumped from the platform onto the train. Our mental scene then goes on to see him falter briefly before regaining his balance and then tipping his hat before jauntily hopping into the train car. As station employees were helping the jaunty man get safely into the train, they inadvertently jostled a package out of the man's grip.[194] The package fell onto the tracks, and the fireworks in the package exploded.[195] The explosion knocked over a set of scales at the other end of the platform.[196] The scales fell and injured the plaintiff as she waited for a later train.[197] In rejecting the argument that the railroad owed the plaintiff a duty to not drop a potentially combustible package, Justice Cardozo wrote that "the orbit of the danger as disclosed to the eye of reasonable vigilance would be the

190. *Id.* at 694.
191. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 41.
192. *Id.* at 43.
193. Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 99 (N.Y. 1928).
194. *Id.*
195. *Id.*
196. *Id.*
197. Waiting for a later train is probably also what the guy with the fireworks should have done. *Id.*

orbit of the duty."[198] It has since become black letter law that a reasonable duty of care is owed to foreseeable plaintiffs.[199]

A. Special Relationships and Duty

The question of who is a foreseeable plaintiff, however, is one that is often hard to answer. In many situations, a duty will not exist unless there is a special relationship between the plaintiff and defendant.[200] Several factors may influence whether a special relationship exists.[201] A defendant who assumes custody or assumes responsibility of something may be held to have a special relationship with the plaintiff.[202] Factors for finding a special relationship may also include the magnitude and likelihood of injury, the burden on defendants to address the risk, and the relevant societal interests.[203] Some states infer the existence of a duty-creating relationship based on certain dynamics, like manufacturer-consumer.[204] In Alaska, the state has a duty to closely supervise parolees in order to protect members of the public.[205] Fox and Stein note that in exceptional cases, a special relationship may also lead to a duty to avoid causing emotional harm to others.[206]

Special relationships are a common way to establish a duty, but they are not the only way. In Minnesota, if the plaintiff's injury is foreseeable and "a direct result of an actor's own conduct," a court might recognize a duty of care even without a special relationship between the parties.[207] The factors of foreseeability and "direct results" both illustrate the frequent overlap between duty and causation most famously demonstrated by *Palsgraf*.

Another major issue related to duty is the extent to which someone has a duty to protect others from third-party criminality. In general, defendants do not have a duty to prevent crime.[208] When there is a special relationship, however, such a duty may be inferred.[209] Common carriers like passenger trains, for instance, have a heightened duty of care toward their riders.[210] Likewise, a

198. *Id.* at 100 ("One who jostles one's neighbor in a crowd does not invade the rights of others standing at the outer fringe when the unintended contact casts a bomb upon the ground.").

199. *See, e.g.*, McDonald, *supra* note 170, at 385 (citing W. Jonathan Cardi, *The Hidden Legacy of Palsgraf: Modern Duty Law in Microcosm*, 91 B.U. L. REV. 1873, 1884 (2011)) ("Forseeability is 'often cited as the most important factor in duty,' and the use of foreseeability in deciding matters of negligence is 'nearly ubiquitous.'").

200. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 41.

201. Pinson, *supra* note 142, at 49.

202. McDonald, *supra* note 170, at 376.

203. Pinson, *supra* note 142, at 49.

204. *See* Moning v. Alfono, 254 N.W.2d 759, 765 (Mich. 1977).

205. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 45.

206. Fox & Stein, *supra* note 27, at 988.

207. McDonald, *supra* note 170, at 367.

208. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1587.

209. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 45.

210. *See* Hines v. Garrett, 108 S.E. 690, 694 (Va. 1921).

landlord can be held liable for injuries if they fail to secure common areas of the property.[211]

Special relationships can also be determinative in other ways. In the case of disclosure of personal information, courts may look for a special relationship between the plaintiff and the audience of the disclosure.[212]

Johnson argues that the situations most strongly supporting a duty to secure information will involve a business relationship between the breached entity and the individual victim.[213] For example, there may be a duty to secure data when there is a fiduciary relationship, as between an insurer and a policy applicant.[214] Simpson notes that if there is no direct relationship, as in the case of a consumer injured by a cyberattack against a payment processor, courts are reluctant to recognize a duty of care.[215] On the other hand, if the defendant's actions created "an unreasonable risk of criminal misconduct," this might create a duty of care towards those who are foreseeably endangered by this conduct.[216]

Rabin proposes two theories of liability for intermediaries that protect personal data: "negligent failure to provide adequate security, and negligent enabling responsibility."[217] Rabin's theory of enabling torts would not require a special relationship to establish that the defendant has a duty when that the defendant has affirmatively enhanced the risk of harm.[218]

B. Creating Duties

A duty may be created by statute or contract, and courts may find a duty based on the facts and precedent.[219] Legal duties are "imposed by law for the protection of potential victims."[220] The Connecticut Supreme Court in *Coburn v. Lenox Homes* stated, "A duty to use care may arise . . . from circumstances under which a reasonable person, knowing what he knew or should have known, would anticipate that harm of the general nature of that suffered was likely to result from his act or failure to act."[221] Torts scholarship often addresses duties and whether a particular duty should exist.[222]

211. *See* Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 487 (D.C. Cir. 1970); Johnson, *supra* note 141, at 23; Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1608.

212. Ludington, *supra* note 62, at 164.

213. Johnson, *supra* note 141, at 24.

214. *See* Daly v. Metropolitan Life Ins. Co., 782 N.Y.S. 2d 530, 534 (Sup. Ct. 2004) (finding a duty to protect confidential information); Johnson, *supra* note 141, at 24; Pinson, *supra* note 142, at 50–51.

215. Simpson, *supra* note 3, at 685–86.

216. Richards & Solove, *supra* note 145, at 1923; *see also* Riedy & Hanus, *supra* note 28, at 29.

217. Rabin, *Data*, *supra* note 129, at 331.

218. Rabin, *Enabling Torts*, *supra* note 182, at 442.

219. *See* Coburn v. Lenox Homes, Inc., 441 A.2d 620, 624 (Conn. 1982); McDonald, *supra* note 170, at 371; Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1586.

220. McDonald, *supra* note 170, at 373 (quoting JOHN C.P. GOLDBERG & BENJAMIN C. ZIPURSKY, THE OXFORD INSTRUCTIONS TO U.S. LAW: TORTS 80 (2010)).

221. 441 A.2d at 624.

222. *E.g.*, Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1571 (suggesting that software manufacturers should have a duty to produce secure software).

Duties can be created or destroyed by statute. Before the USA PATRIOT Act, some litigants had argued that software manufacturers should be held liable for harmful software bugs under the Computer Fraud and Abuse Act, but then the CFAA was amended to remove this option for liability.[223] The Communications Decency Act of 1996 ("CDA") protects ISPs from an unpredictable legal environment by not holding the ISPs responsible for defamatory statements on the websites they host.[224] Both of these examples can be viewed as statutory changes that remove a disputed duty. The liability of software manufacturers is often reduced or eliminated by contract, and the amendments to the CFAA clarified that the CFAA was not a statutory source for a duty to produce secure software. Similarly, the CDA establishes that ISPs have no duty to protect the public from the content of their sites.[225]

The GLBA and HIPAA are federal laws that impose a duty to secure data.[226] These two laws thus apply to a lot of data breach incidents, as Advisen data indicates that the finance and insurance industry suffered 5,512 data breach incidents between 2005 and 2014, and the healthcare industry suffered 4,136 data breach incidents during the same timeframe. Yet a duty to secure data should be broad, predictable, and not limited by the patchwork nature of information privacy laws in the United States. Between 2005 and 2014, the information technology industry experienced 1,446 data breach incidents affecting over 10 billion records, significantly more than the 1.56 billion records for the finance and insurance industry and the 1 billion records for the healthcare industry. Even still, there is no analogous federal law imposing a duty to secure data on the information technology industry, even though passwords and email accounts are increasingly useful tools for cyber criminals.

One of the key aspects of the arguments over duty is the distinction between nonfeasance and misfeasance, or passive inaction versus active misconduct.[227] If there is a special relationship between the defendant and the plaintiff, like a landlord-tenant relationship, nonfeasance may be enough to hold the defendant liable.[228] Nonfeasance also may support liability in the presence of prior incidents like the cause of the present injury.[229] Rabin also notes that some courts may recognize a duty to act for the protection of third parties when the nature of the environment creates an "especial temptation" for a would-be criminal.[230]

223. *See supra* note 68 and accompanying text.

224. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 97–98.

225. *Id.* at 104 ("Immunity is breeding irresponsibility because websites have no incentive or duty to protect their visitors and the general public."). This aspect of the CDA was amended slightly in 2018 to remove immunity for websites that knowingly assist, facilitate, or support sex trafficking. Pub. L. 115-164, H.R. 1865 (2018); Emily Stewart, *The Next Big Battle Over Internet Freedom Is Here*, VOX (Apr. 23, 2018, 12:20 PM), https://www.
vox.com/policy-and-politics/2018/4/23/17237640/fosta-sesta-section-230-internet-freedom.

226. *See supra* Subsection II.C.1.

227. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 42; McDonald, *supra* note 170, at 369.

228. Rabin, *Enabling Torts*, *supra* note 182, at 444.

229. *Id.* at 445.

230. *Id.* at 446.

In the 1830 case *Patapsco Insurance Co. v. Coulter*, the Supreme Court evaluated a dispute involving marine insurance where the insured lost a vessel and its contents in a fire at a foreign port.[231] The issue of misfeasance versus nonfeasance arose because the entire ship evacuated very early after the fire started, due to the presence of gunpowder in the ship's cargo.[232] One of the legal questions concerns whether the captain and crew had an obligation to make efforts to extinguish the fire before abandoning the ship.[233] The Supreme Court explored several similar cases and noted that some nonfeasances actually involve misfeasances "because they violate implied duties incident to navigating the vessel, and produce a positive and definite increase of risk."[234] This case illustrates the principle that in some situations, a failure to act may be a misfeasance.

It may be more difficult to distinguish between misfeasance and nonfeasance in cases involving third-party criminality. Consider a fact pattern where a gun shop owner inadequately secures the shop and its inventory, and a thief steals a gun and murders someone. McDonald notes that a failure to secure in such a situation has been found to be an inactionable, passive choice in one jurisdiction, and affirmative conduct in another.[235]

The misfeasance/nonfeasance distinction raises difficult questions in the context of data insecurity injuries. If one does not maintain a secure computer network, is that an act, or a failure to act? In an environment where security is tacked on as an afterthought, failure to add security is a failure to act. But if security is an essential aspect of building and maintaining the network, the conscious act of not taking security measures could be characterized as misfeasance instead of nonfeasance. In the data injury context, issues of security and duty will thus necessarily be tied to a question of social and professional norms.

There are arguments to support an implied duty based on norms. In the *Patapsco Insurance* case, the Court considered whether trying to extinguish a fire before abandoning a ship was one of the "implied duties incident to navigating the vessel."[236] In the context of data injuries, an analogous question would ask whether security is an implied duty incident to maintaining a large database of sensitive personal information. To the extent that security is an essential element, failing to secure one's networks can be a misfeasance under the reasoning in *Patapsco Insurance*.[237]

There is a potentially broader argument based on the essential nature of access controls in database management. If everyone could access everything, data breaches would not really exist, because neither does privacy. Instituting access controls for the data is an affirmative act. As the decision to adopt *any*

231. 28 U.S. 222, 228 (1830).
232. *Id.* at 223–24.
233. *Id.* at 229.
234. *Id.* at 235.
235. McDonald, *supra* note 170, at 381–82.
236. *Patapsco*, 28 U.S. at 235.
237. *See generally id.*

security measure is an affirmative act, negligent actions during the creation and implementation of a security system are appropriately categorized as misfeasance. In the interest of legal consistency and clarity, however, we prefer the *Patapsco* approach.

C. Digital Duties

Rustad and Koenig compare a duty to protect users from cyber criminals to the concept of premises liability.[238] Under a premises liability theory, when a property owner welcomes the general public for business purposes, those customers become invitees and entitled to some level of protection from possible hazards.[239] The negligent failure to provide adequate security tort focuses on the relational obligations of the defendant in deciding whether they had a duty to provide adequate security.[240] A landlord-tenant relationship is one example. In *Kline v. 1500 Massachusetts Avenue Apartment Corp.*, the D.C. Circuit established that landlords have a duty to minimize risk in common areas.[241]

Technology also introduces opportunities to reexamine previous standards of reasonableness in determining the presence of a duty. Under the federal Economic Espionage Act ("EEA"), data owners must take reasonable measures to protect secrecy in order to meet the definition of a trade secret.[242] Rowe analyzes trade secret law in the context of technological developments to examine if the concept of "reasonable efforts" should be reevaluated due to the increased risk of trade secret theft enabled by new technologies.[243]

Before state data breach laws were widely enacted, some commentary considered two main possibilities: (1) recognizing an obligation to secure the personal information of others and (2) recognizing an obligation to disclose data breaches.[244] Data breach laws overwhelmingly favor the second option. It has been ten years since state data breach laws started to become more common. If the obligation to disclose has not increased social welfare, perhaps the law should instead support an obligation to secure.

Currently, data breach laws in the United States are first and foremost about transparency. The common model is as follows: When a company that does business in a state experiences a data breach, they have to notify affected consumers.[245] If the breach affects more than a threshold number of state residents, the breached business must often notify another party too, like the state Attorney General's office or a credit reporting agency.[246] Often, the notification requirement is conditioned on the stolen information being unencrypted. Some

238. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1581.
239. *Id.* at 1581–82.
240. Rabin, *Data*, *supra* note 129, at 331.
241. 439 F.2d 477, 488 (D.C. Cir. 1970); Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1584.
242. 18 U.S.C. § 1839(3)(A) (2018); Rowe, *supra* note 1, at 8.
243. Rowe, *supra* note 1, at 3.
244. Johnson, *supra* note 141, at 22.
245. *E.g.*, CAL. CIVIL CODE § 1798.29(a) (West 2017).
246. *E.g.*, *id.* § 1798.29(e).

data breach laws state that a violation of the statute is also a violation of state consumer protection law.[247] Some data breach statutes address civil liability for violations, but many others do not.[248] Generally though, the scope of a duty created by a data breach notification law will be limited to the duty to notify affected individuals after a breach. Illinois courts have found that if the notification requirement is complied with, the statute has not been violated.[249] Such data breach laws thus create a duty to *notify* customers of data breaches but do not typically create a duty to *prevent* data breaches.[250]

Data breach notification statutes are consistent with the legal system's treatment of failures to warn about dangerous conditions.[251] With data breach notification statutes, however, the dangerous conditions only exist in the aftermath of a data breach. Data breach laws, in other words, impose a duty to warn when data is stolen, and say nothing about the dangerous conditions created by bad security practices.

Sometimes after a data breach, stolen information is published to a wide audience, as in the case of the hack of the adultery-friendly dating website Ashley Madison.[252] The data thieves ultimately published the data, a practice that has come to be called organizational doxing.[253] Oldberg argues that when organizations are entrusted with such personal information, this place of trust that they hold leads to "a duty . . . to keep that data private."[254]

In taking on information security obligations, organizations commit to protecting the confidentiality, integrity, and availability of the data they host.[255] It is reasonable to read a duty of care into this relationship. Ludington, in considering the contours of such a duty, suggests the application of Fair Information Practices, four principles restated in various forms in several government agencies and in the Privacy Act of 1974.[256] A duty is also supported by statutory trends towards liability for upstream and downstream participants in data theft.

247. *E.g.*, 815 ILL. COMP. STAT. 530/20 (2006) ("A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.").

248. Johnson, *supra* note 141, at 22.

249. Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 28 (Ill. App. Ct. 2010).

250. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 101–02; *see also* Waers, *supra* note 88, at 51 (discussing a data breach of medical records where the data was not misused).

251. Johnson, *supra* note 141, at 26.

252. Sara Malm, *Two Suicides Are Linked to Ashley Madison Leak*, DAILYMAIL (Aug. 24, 2015, 9:59 AM), http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html.

253. Oldberg, *supra* note 48, at 186.

254. *Id*.

255. *See* Riedy & Hanus, *supra* note 28, at 10 ("The term 'information security' comprises three interrelated components: confidentiality, integrity, and availability of data.").

256. Ludington, *supra* note 62, at 146.

D. Duty and Psychology

Duty is more than mere obligation. When a duty is recognized under the law, that recognition is grounded in the concept of fairness, and the goal is to fairly distribute liability burdens. Fairness, however, is difficult to quantify. This Section uses a combination of legal theory and behavioral science to provide insights about legal duties.

Rawlsian conceptions of justice emphasize justice as fairness, with the principles being determined by how a rational person in an "original position" would shape society if they acted without concern for their own status.[257] The veil of ignorance is essential for Rawls's original position, which requires the rational person to be ignorant of their own class position, their own skills, and any quirks of the rational person's individual psychology like that person's aversion to risk.[258] Analysis through the veil of ignorance can consider human psychology generally.[259]

In data breaches, the breached entity is typically in the best position to know of its own security strengths and weaknesses and thus act for the protection of its customers. Unfortunately, cognitive biases are in play, which often lead to people underestimating the risk of a disaster. To reach an "original position" on duties in data security law, we must first identify the biases that prevent a truly objective analysis.

In the book *The Ostrich Paradox*, Meyer and Kunreuther discuss six biases that people encounter when dealing with risks.[260] These biases are Myopia, Amnesia, Optimism, Inertia, Simplification, and Herding.[261] Cognitive biases often contribute to poor judgment and adverse outcomes. To illustrate the six biases, the authors use six examples that resulted in serious losses.

Myopia. Thailand officials chose to not build sirens along the coasts in case of tsunamis because of the possible effects on tourism.[262] In 2004, the Indian Ocean Tsunami killed thousands of people, some of whom might have been saved if an early warning system had been in place.[263]

Amnesia. The Japanese village of Miyako has been destroyed multiple times by tsunamis, but each time it was rebuilt, people resettled along the bay.[264] Over 4,000 structures were destroyed by a tsunami in 2011.[265]

257. Kenneth Einar Himma, *Privacy Versus Security: Why Privacy Is Not an Absolute Value or Right*, 44 SAN DIEGO L. REV. 857, 891–92 (2007).

258. Stephen M. Griffin, *Reconstructing Rawls's [sic] Theory of Justice: Developing a Public Values Philosophy of the Constitution*, 62 N.Y.U. L. REV. 715, 734 (1987).

259. *Id.*

260. ROBERT MEYER & HOWARD KUNREUTHER, THE OSTRICH PARADOX: WHY WE UNDER PREPARE FOR DISASTERS 12 (2017).

261. *Id.*

262. *Id.*

263. *Id.* at 13–14.

264. *Id.* at 22.

265. *Id.* at 21.

Optimism. Larry Silverstein acquired the twin towers of the World Trade Center ("WTC"),[266] but underestimated the terrorism risk. Soon after the acquisition, the buildings collapsed in the 9/11 terrorist attack.[267]

Inertia. In 2004, the city of New Orleans was nearly hit by Hurricane Ivan, which exposed many weaknesses in the city's preparedness against large hurricanes.[268] The city officials did not know how to improve resiliency with a tight budget, so they chose not to do anything. The city suffered a huge loss after Hurricane Katrina in 2005.[269]

Simplification. Motorcyclists are killed every year because they were not wearing a helmet when they had an accident.[270] People often ignore probabilities when making decisions because probabilities are complex and abstract, and the mind favors simplicity.[271]

Herding. In 1977, a fire broke out at the Beverly Hills Supper Club in Kentucky.[272] A bus boy got up on stage and announced that there was a fire and everyone should exit the building.[273] There was a delay while many of the audience members looked around to see whether others were evacuating, and 165 people perished in the fire.[274]

As the authors argued, these biases are embedded in our subconscious and discourage us from making optimal risk management decisions if we do not correct them deliberately.

These biases also affect how individuals and organizations manage cyber risks. In May 2017, government hospitals in the United Kingdom were hit by the WannaCry ransomware attack, causing thousands of operations and appointments to be cancelled.[275] WannaCry took advantage of a security flaw that Microsoft had patched in March 2017. Yet 90% of the National Health Service ("NHS") hospitals still used computers that ran Windows XP, and Microsoft had stopped supporting security updates for Windows XP in 2014.[276]

Several cognitive biases can be seen at play in the hospitals' security failures during the WannaCry attack. Hospital administrators showed the Optimism bias by underestimating the risk of being attacked. The Myopia bias is connected to the failure of the hospitals to prioritize cybersecurity improve-

266. *Id.* at 31.
267. *Id.* at 32.
268. *Id.* at 43.
269. *Id.* at 43–44.
270. *Id.* at 53.
271. *Id.* at 54.
272. *Id.* at 59.
273. *Id.*
274. *Id.* at 59–60.
275. Alexander Smith et al., *Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.*, NBC NEWS (May 17, 2017, 8:39 AM), https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126.
276. Laura Donnelly & Ben Farmer, *NHS Repeatedly Warned to Improve Security, Defence Secretary Says*, TELEGRAPH (May 17, 2017, 10:00 PM), http://www.telegraph.co.uk/news/2017/05/14/nhs-repeatedly-warned-improve-security-defence-secretary-says/; Smith et al., *supra* note 275.

ments over other short term objectives. The Inertia bias also appears because some of the hospitals saw that security should be a priority, but when faced with a difficult choice, they often resorted to the default condition, which was inaction.

This Section is mostly concerned with how cognitive biases influence the risk management process. Risk management starts with the identification of a problem. This process has many intermediate steps. In the book *Principles of Risk Management and Insurance*,[277] the author, George Rejda, describes a four-step risk management process as consisting of:

Identify. Identify potential losses.[278]

Analyze. Measure and analyze the loss exposures.[279]

Treat. Select the appropriate combination of techniques for treating the loss exposure.[280]

Monitor. Implement and monitor the risk management program.[281]

There are many other ways of describing the process, such as the standard ISO 31000 "Risk management—Principles and guidelines on implementation" consisting of seven risk management steps.[282] The ISO 31000 recommendations generally fit into Rejda's four-step framework, plus some additional details and features. Communication and consultation occur throughout the process.

TABLE 1: RISK MANAGEMENT

<table>
<tr><th>Rejda 4-step process</th><th colspan="2">ISO 31000 7-step process</th></tr>
<tr><td rowspan="2">Identify</td><td>Establish the context</td><td rowspan="5">Communication and consultation</td></tr>
<tr><td>Risk identification</td></tr>
<tr><td rowspan="2">Analyze</td><td>Risk analysis</td></tr>
<tr><td>Risk evaluation</td></tr>
<tr><td>Treat</td><td>Risk treatment</td></tr>
<tr><td>Monitor</td><td>Monitoring and review</td></tr>
</table>

277. GEORGE D. REJDA & MICHAEL J. MCNAMARA, PRINCIPLES OF RISK MANAGEMENT AND INSURANCE 48–49 (13th ed. 2016).

278. *Id.* at 48.

279. *Id.*

280. *Id.* at 49.

281. *Id.*

282. *See* INT'L ORG. FOR STANDARDIZATION, ISO 31000, RISK MANAGEMENT—PRINCIPLES AND GUIDELINES (2009).

Our risk management process has five steps instead of Rejda's four or ISO's seven. The first two steps of ISO 31000 are arguably both included within Rejda's conception of identifying the risk and can be consolidated into one step. On the other hand, the distinction that ISO 31000 makes between risk analysis and risk evaluation is insightful. Analysis results in the risk becoming understood, and evaluation results in the risk being ranked alongside other priorities. In the Indian Ocean Tsunami incident, Thailand officials apparently analyzed and understood the impacts a tsunami could have, but their evaluation of the risk was that addressing the risk was not as important as protecting the tourism industry. Thus, we describe a risk management process as follows:

Identify. Risk managers recognize and define a risk.

Analyze. Risk managers determine the severity of the risk.

Evaluate. Risk managers determine the importance and urgency of the risk relative to other tasks.

Treat. Risk managers make decisions on risk management strategies (retention, avoidance, mitigation, or transfer), implement actionable plans, and execute.

Review. Risk managers keep monitoring the risk and repeat the previous steps if there are any changes to the risk.

In order to understand the roles that the biases play in this process, again, we look at the six incidents described in *The Ostrich Paradox*.[283] We impose the five-step risk management process on them as an extra dimension so that we can see how the biases cause it to fail at different stages.

In Table 2, the failing points of the risk management process are marked in dark gray. Light gray cells indicate risk management steps that were successfully followed. Please note that each incident is not necessarily caused by only one bias. In 2005, with Hurricane Katrina, it was very likely that the city of New Orleans was underprepared not only due to Inertia, but also because officials underestimated the probability of experiencing catastrophic hurricanes in two successive years (Optimism), or they did not want to invest in protection when they could spend the money elsewhere (Myopia). We only highlight the one that is most strongly associated with each incident. From the table, we find that every step in this process is vulnerable, and there is a causal relationship between the six biases and risk management failures.

Risk identification failure. People do not have enough information about their situation, and thus ignore the surrounding risks (Simplification).

Risk analysis failure. The possibility of disaster occurring is underestimated (Optimism).

Risk evaluation failure. Risk management is not given enough priority because people focus too much on short-term objectives (Myopia).

283. MEYER & KUNREUTHER, *supra* note 260, at 12.

Risk treatment failure. People do not implement risk mitigation strategies either because they are reluctant to change (Inertia), or due to a social norm that people do not treat the risk (Herding).

Risk review failure. People forget to keep monitoring a risk if the risk has not materialized for a long time (Amnesia).

Therefore, to mitigate the negative effects brought by the six biases, we should ensure the quality of every step in the risk management process. When dealing with cyber risks, this can be achieved through a legal duty to secure as mentioned earlier.

TABLE 2: COGNITIVE BIASES AND RISK MANAGEMENT

Bias	Incident	Risk Management Process				
		Identify	Analyze	Evaluate	Treat	Review
Myopia	Thailand in Indian Ocean tsunami 2004	Risk was successfully identified by Thailand's department of meteorology	People understood tsunami risk could be devastating	Officials failed to prioritize mitigating tsunami risk when there was an upfront cost.	No treatment	No review
Amnesia	Miyako in earthquake and the following tsunami 2011	The risk of earthquake and tsunami was identified by ancestors in that area	People knew the consequences well from disasters in the past	Ancestors saw the importance in avoiding the risk	Monuments were built to remind people to avoid the hazard zone	Residents failed to monitor the risk and keep enforcing the risk avoidance plan
Optimism	Larry Silverstein's acquisition of WTC before 9/11 2001	WTC had a history of being attacked by terrorists, and a report identified the terrorism risk before acquisition	Larry and insurers underestimated the probability of being attacked again	No evaluation	No treatment	No review

Inertia	New Orleans in Hurricane Katrina 2005	The city of New Orleans identified the risk of being hit by hurricanes	The city officials estimated the severity of a catastrophic hurricane from Hurricane Ivan in 2004	The city realized it was underprepared for large hurricanes due to weaknesses, which were also known	The city failed to take actions to improve preparedness when there was a dilemma	No review
Simplification	Rate of motorcyclists who ride without helmets	The abstract concept of probability of harm leads to risks not being identified.	No analysis	No evaluation	No treatment	No review
Herding	Audience in the Beverly Hill Supper Club fire 1977	The fire was identified	People found that the fire was nearby and could not be controlled	Urgency of the situation was told to the audience	Audience failed to escape immediately. They wanted to follow others, but no one was taking any actions	No review

FIGURE 4: THE RISK MANAGEMENT CYCLE AND COGNITIVE BIASES

One of the ways to address problems at the identification stage is to create a risk bundle. That is, pair the abstract and hard to predict risk with a more concrete risk, like legal liability. Legal risk is often more visible to managers of an organization. When legal risk is bundled with the underlying risk, addressing the legal risk can improve both risks. This does not necessarily mean that the Simplification bias is overcome, but the threat of legal liability should deter some people from underestimating the risk. According to the statistics from the Insurance Institute for Highway Safety and the Highway Loss Data Institute, in 2016, helmet wearers made up 60% of all motorcycle fatalities. In states with no law requiring motorcyclists to wear helmets, though, only 27% of those fatalities involved victims who were wearing a helmet.[284] This suggests that in states with no helmet laws, the temptation to not use a helmet may be stronger. By tying legal risk to a more abstract, probability-based risk, legal policy can help risk managers avoid the Simplification bias as it becomes less likely that people will ignore the risk.

The interactions between cognitive biases and the risk management process indicate that some legal intervention could be appropriate in order to support objective analysis. In such a situation, creating a legal duty to act could control for some of the cognitive biases that complicate risk management. This would be especially valuable in the network security context, where risk management is central.

IV. INJURY AND REMEDIES

Tort law in the United States originally emphasized injury to the physical body. Recognition of emotional or less overtly physical harms came later. There were a few early intentional torts without physical harm requirements, like false imprisonment. Goldberg points out that harms from false imprisonment were not cast as emotional harms but rather as violations of a liberty.[285] Likewise, injuries from defamation were characterized as reputational injuries.[286] The person who suffers these injuries had encountered interference with the essential right to self-determination, because they lost control over where they could go (false imprisonment) or how they were represented to others (defamation).

In the aftermath of a cyberattack, victims often worry about lost profits. We argue that data injuries have more in common with false imprisonment than they do with lost profits. Such injuries are the result of a third party exercising control over an important aspect of oneself. Data injuries are not harms to the physical body but are instead violations of the right to control the known aspects of one's identity. Torts applicable to data breaches and other cybersecuri-

284. *Motorcycles (2016)*, INS. INST. FOR HIGHWAY SAFETY AND THE HIGHWAY LOSS DATA INST. (Dec. 2017), http://www.iihs.org/iihs/topics/t/motorcycles/fatalityfacts/motorcycles.

285. Goldberg, *supra* note 137, at 819.

286. *Id.* at 824.

ty events are likely to involve financial injuries, dignitary injuries, and privacy injuries.[287] Unfortunately, in the area of remedies, courts are often ill-prepared to address injuries that cannot be observed.

One of the underlying questions about data is what kind of interest the originating individual has in it. The nature of this interest should influence how this interest is treated. In John Locke's *Second Treatise of Government*, Locke famously argues that a person acquires property rights through their labor, including the improvement of natural resources.[288] An individual's raw data is generally not worth much before it is commodified by a third party like a data broker, so if anyone should have a Lockean property right in data, it is probably the data brokers.

James Madison took a broader view of property as including not just land and material goods but also "[one's] opinions and the free communication of them."[289] Madison wrote that the purpose of government is "to protect property of every sort," and that a just government is one "which *impartially* secures to every man, whatever is his *own*."[290] Still, as our legal system is very preoccupied with economically quantifiable rights, a Madisonian approach to property in one's being and the associated information may not be well-suited to the court system.

A. Injuries

There is a clear need for the legal system to evolve in its handling of injuries. The legal system primarily exists to address harms within a community. Solove and Citron define harm as "the impairment, or set back, of a person, entity, or society's interests."[291] Data insecurity frequently impairs important interests, but it does not easily fit within existing concepts of injury. This Section evaluates modern legal injuries and asks what improvements should be made to better account for modern harms.

Tort law has come a long way from its earlier focus on physical injuries, and science is likely to help continue that pattern. Recent research has examined the interaction between bodily states and emotions. Physical warmth may prime feelings of interpersonal warmth, for example.[292] Goldberg examines the

287. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1603.

288. JOHN LOCKE, TWO TREATISES OF GOVERNMENT 129 (Edward J. Harpham ed., Univ. Press of Kan. 1992) (1960) ("God gave the world to men in common for their use. Men own themselves, and by extension they own their own labor. They create property by mixing their own labor, which is unconditionally their property, with unowned common resources, thereby creating something new, which becomes their property as well (*ST*: no. 27).").

289. James Madison, *Property*, THE FOUNDERS' CONSTITUTION (1792), http://press-pubs.uchicago.edu/founders/documents/v1ch16s23.html.

290. *Id.* Of course, Madison's theories of property are inherently flawed, as he supported chattel slavery, making this quote very suspect in hindsight.

291. Solove & Citron, *supra* note 27, at 747.

292. Adam Benforado, *The Body of the Mind: Embodied Cognition, Law, and Justice*, 54 ST. LOUIS U. L.J. 1185, 1205 (2010).

continued need for treating physical and emotional injuries differently in the law, even as neuroscientists demonstrate frequent spots of overlap.[293]

The subjectivity of injuries can create challenges for tort theory. With emotional injuries, the court is often asked to take the plaintiff's word about psychological and emotional impacts.[294] Even with physical injuries, pain cannot be measured directly and thus has a strong inherently subjective element.[295]

Characterizations of injury tend to emphasize physical harms, especially easily observable harms.[296] Persad instead frames injuries as mind-dependent and mind-independent.[297] One seemingly far-fetched example that Persad gives is of malicious actors using flashing images to trigger a seizure in someone with epilepsy.[298] The trigger is communicative, not physical, but the injury is potentially serious.

As it turns out, Persad's scenario was not far-fetched at all. Such an attack was perpetrated against Newsweek journalist Kurt Eichenwald in December of 2016 when an Internet troll attempted to flood his Twitter feed with animated GIFs.[299] The flashing images triggered an eight minute seizure.[300] A grand jury returned an indictment against the suspect, John Rayne Rivello, for assault with a deadly weapon.[301] He was also charged with the federal crime of cyberstalking, though that charge was dismissed in November of 2017.[302]

Earlier cases have generally rejected allegations of harm caused by words or pictures.[303] In *Winter v. G.P. Putnam's Sons*, plaintiffs sued a book publisher for products liability.[304] Plaintiffs had relied on the defendant's publication when foraging for mushrooms, but the book had some flaws in that the most deadly species of mushrooms were not adequately described. Both plaintiffs became critically ill and had liver transplants as a result.[305] The court held that a book's contents are not an appropriate source for products liability, and that a publisher had no duty to verify the accuracy of its publications.[306]

293. Goldberg, *supra* note 137, at 809.

294. Fox & Stein, *supra* note 27, at 991; Solove & Citron, *supra* note 27, at 767 (noting that emotional distress claims are criticized as being too easy to fake).

295. Amanda C. Pustilnik, *Pain as Fact and Heuristic: How Pain Neuroimaging Illuminates Moral Dimensions of Law*, 97 CORNELL L. REV. 801, 803 (2012). Pustilnik also observes that because of the way that the brain processes nociception transmissions, "without consciousness, there is no pain." *Id.* at 808.

296. Govind Persad, *Law, Science, and the Injured Mind*, 67 ALA. L. REV. 1179, 1181 (2016).

297. *Id.* at 1183.

298. *Id.* at 1184–85.

299. Mary Emily O'Hara, *Kurt Eichenwald Case: Texas Grand Jury Says a GIF Is a 'Deadly Weapon'*, NBC NEWS (Mar. 21, 2017, 2:38 PM), https://www.nbcnews.com/news/us-news/kurt-eichenwald-case-texas-grand-jury-says-gif-deadly-weapon-n736316.

300. Joshua Rhett Miller, *Vet Accused of Sending Reporter Seizure-Causing Tweet Catches Small Break*, N.Y. POST (Nov. 28, 2017, 12:58 PM), https://nypost.com/2017/11/28/vet-accused-of-sending-reporter-seizure-causing-tweet-catches-small-break/.

301. O'Hara, *supra* note 299.

302. *Id.*

303. Persad, *supra* note 296, at 1192.

304. 938 F.2d 1033, 1034 (9th Cir. 1991).

305. *Id.*

306. *Id.* at 1036.

In the *Rivello* prosecution, the court is evaluating electronic communications as a weapon.[307] The case has more in common with data misuse than it does with data breaches, but it has potential applications for both of these causes of digital injuries. Epilepsy cases may lead to liability for other injuries like intentionally triggering a dissociative episode for a sufferer of posttraumatic stress disorder. More relevant for our purposes, if electronic communications are recognized for their destructive potential, this supports recognition for data insecurity injuries.

For reasons difficult to articulate, data breaches offend social order. Society recognizes that theft is wrong. But theft is about things, and data breaches are often about people. The injury is harder to observe. Injuries caused by data breaches are often more psychological in nature, like apprehension of future injuries.[308] Solove and Citron describe data breach harms as "intangible, risk-oriented, and diffuse."[309] Moreover, judges addressing these harms may view the task as being like trying to "tap dance on quicksand."[310] Many times, the proffered argument for recognizing data breach harm is criticized as being too speculative.[311]

Courts usually focus on financial injuries in data breach cases, but even in cases where individuals experience credit card fraud, the card issuers typically absorb the loss.[312] Identity theft can be costly to fix,[313] but plaintiffs who have not yet suffered identity theft have not taken on those costs.[314] Most individual victims will have paid, at most, for credit monitoring and other minor transactional costs.[315] Multiple courts have rejected the premise that loss of data, without actual identity theft, results in a legally recognizable injury.[316] Some argue that the rate of actual identity theft is low in relation to the number of data breaches, suggesting that data breach victims are not often also identity theft victims.[317] At the same time though, one study found that two-thirds of identity theft victims had also received a notification that their information was included in a data breach.[318] So most data breach victims may not be identity theft victims, but most identity theft victims are also data breach victims.

307. O'Hara, *supra* note 299.

308. Rabin, *Data*, *supra* note 129, at 315; Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1603.

309. Solove & Citron, *supra* note 27, at 737.

310. *Id.* at 744.

311. Riedy & Hanus, *supra* note 28, at 7–8.

312. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1603.

313. Johnson, *supra* note 141, at 27. *But see* Riedy & Hanus, *supra* note 28, at 18–19 (citing identity theft statistics from 2014, when most out-of-pocket losses were less than $99, and only 14% of identity theft victims had costs of $1,000 or more).

314. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1603.

315. Rabin, *Data*, *supra* note 129, at 333.

316. Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006); *see also* Pinson, *supra* note 142, at 56; Romanosky, Hoffman & Acquisti, *supra* note 30, at 92 (noting that data breach lawsuits without "actual harm" are often dismissed); Simpson, *supra* note 3, at 686; Waers, *supra* note 88, at 51 ("Most jurisdictions require actual damages to be present to succeed on an action for negligence in data management."); Wooten, *supra* note 113, at 232.

317. Riedy & Hanus, *supra* note 28, at 16–17.

318. *Id.* at 32–33.

We argue that past courts have been too focused on monetary injuries. The main offense caused by data breaches is a violation of privacy. The injury is often emotional in nature, as data breaches can cause people to experience fear and anxiety.[319] There are numerous studies conducted across gender, age, and cultural lines demonstrating the psychological anxiety and stress caused by data breaches and online identity theft, including showing an increase in maladaptive psychological and somatic symptoms post-victimization among victims of identity theft.[320] Solove and Citron discuss the fear and anxiety aspects of data injuries at length.[321] In characterizing risk and anxiety as distinct injuries, they shift the goal post for a standing analysis. Instead of asking whether risk and anxiety are injuries, then, courts would ask whether the plaintiff's risk and anxiety injuries were sufficiently severe.

Data misuse arguably causes a more pure injury to autonomy than a data breach. At least when a data breach occurs, the criminality of the behavior and its ramifications are relatively unambiguous. Through animated gifs, social media platforms like Facebook and Twitter enable users to express themselves dynamically using moving pictures as responses. And yet this feature, used maliciously, forced a journalist to experience an eight-minute seizure.[322] In his attack on Eichenwald, John Rivello took advantage of legal ambiguity about electronic stimuli to inflict a medical injury on another person.[323] Meanwhile, Cambridge Analytica used the collective knowledge of millions of Facebook profiles to shape political advertisements in a sordid manipulation of consumer psychology principles.[324]

One reason that we chose to use a negligence framework is that the type of privacy violation caused by data breaches and data misuse often does not fit into the legal framework for privacy torts.[325] Oldberg suggests that the solution might be to adopt a broader right to privacy as envisioned by Warren and

319. Jon D. Elhai & Brian J. Hall, *Anxiety About Internet Hacking: Results from a Community Sample*, 54 COMPUTERS IN HUM. BEHAV. 180, 183 (2016) (reporting results of a survey measuring self-reported anxiety levels about various data breach related topics and finding "data breach" anxiety to have greater severity than resting anxiety); Sushma Sanga & Ali Eydgahi, *Factors Affecting Identity Theft Anxiety Level in College Students* (Am. Soc. for Engineering Educ. 2017, Paper No. 19812), https://www.asee.org/public/conferences/78/papers/19812/view (studying the factors influencing the anxiety caused by fear of identity theft among students in Michigan).

320. *See generally* Karen Reilly & Gráinne Kirwan*, Online Identity Theft, An Investigation of the Differences Between Victims and Non-victims with Regard to Anxiety, Precautions and Uses of the Internet*, *in* CYBERPSYCHOLOGY AND NEW MEDIA: A THEMATIC READER ACCOUNT (Andrew Power & Gráinne Kirwan ed., 2014) (studying the after-effects of being a victim of online identity theft and showing victims of online identity theft experience higher levels of anxiety compared to nonvictims); Jon D. Elhai et al., *Cross-cultural and Gender Associations with Anxiety about Electronic Data Hacking*, 70 COMPUTERS IN HUM. BEHAV. 161 (2017) (studying the impact of data hacking on clinical anxiety and worry among American and Korean men and women); Tracy Sharp et al., *Exploring the Psychological and Somatic Impact of Identity Theft*, 49 J. OF FORENSIC SCI. 1 (2004) (showing an increase in maladaptive psychological and somatic symptoms post-victimization among victims of identity theft).

321. Solove & Citron, *supra* note 27, at 753.

322. *See generally* Miller, *supra* note 300; O'Hara, *supra* note 299.

323. O'Hara, *supra* note 299.

324. *See* Chen & Potenza, *supra*, note 16.

325. Oldberg, *supra* note 48, at 204.

Brandeis in their seminal work on the topic.[326] Ludington goes further and proposes that the misuse of the personal information of others is an injury to autonomy because the individual is being denied the right to choose what information to reveal or keep hidden.[327] This kind of injury is consistent with the values of liberty and reputation that have long been recognized in tort law.

Financial awards cannot truly compensate for autonomy injuries or emotional injuries. After a data breach, individuals may experience anxiety and the fear that they will eventually be injured by identity theft or some other form of fraud.[328] Data insecurity fears also go beyond the financial. Consider, for example, citizens of countries that criminalize homosexuality. An electronic posting about a citizen's sexual orientation in such a country can put individuals at significant legal risk. Some commentary has compared data insecurity injuries to medical monitoring cases.[329] Exposure to toxic substances like asbestos, for example, may result in cancer that doesn't show up until years after the exposure has ended.[330]

The conversation about data insecurity injuries frequently turns back to risk, which is often visualized along an axis of low probability to high probability, and low magnitude of harm to high magnitude of harm.[331] Solove and Citron compare the increased risk of identity theft as being like an increased risk of contracting a chronic disease.[332]

Rabin, however, is skeptical about the application of these principles to data insecurity injuries.[333] In *Stollenwerk v. Tri-West Health Care Alliance*, the Ninth Circuit was likewise unconvinced that medical monitoring cases provided a sufficient analogy for data breach harms.[334] In *Caudle v. Towers, Perrin, Forster & Crosby*, on the other hand, the district court did apply the principles of medical monitoring cases, reasoning that fear of future identity theft could be compared to such cases when there is a rational basis for the fear.[335] The *Caudle* court also provided three factors that may "giv[e] rise to a demonstrable basis for a serious concern over misuse" of the stolen data: (1) lack of password-protection in the case of stolen hardware, (2) evidence that the data thief had the motivation and ability to access the data, and (3) evidence of actual misuse of information included in the breach, whether that misuse affected the plaintiff or someone else in the database.[336]

326. *Id*.

327. Ludington, *supra* note 62, at 147.

328. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1603; Solove & Citron, *supra* note 27, at 747.

329. Cave, *supra* note 113, at 769; Johnson, *supra* note 141, at 29; Martecchini, *supra* note 20, at 1491–92; Rabin, *Data*, *supra* note 129, at 333–34; Solove & Citron, *supra* note 27, at 761–62.

330. Rabin, *Data*, *supra* note 129, at 333–34; Fox & Stein, *supra* note 27, at 985.

331. Solove & Citron, *supra* note 27, at 774.

332. *Id.* at 772.

333. Rabin, *Data*, *supra* note 129, at 334.

334. 254 F. App'x 664, 665 (9th Cir. 2007); *see also* Martecchini, *supra* note 20, at 1491–92; Pinson, *supra* note 142, at 46–47 (discussing the district court decision in Stollenwerk).

335. 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008).

336. *Id.* at 282; *see also* Martecchini, *supra* note 20, at 1493.

Courts generally view data harms very narrowly, requiring such harms to be observable and measurable.[337] Solove and Citron compare data breach harms to "invisible objects in the middle of a crowded room" that can only be "seen" by observing activity in response to its presence.[338] In a 2010 article, Richards and Solove suggest that the law should expand to take intangible harms into account, including harm from the disclosure of non-embarrassing personal information.[339]

As noted above, there is a general uncertainty about whether data insecurity injuries are legally cognizable injuries. In claims based on negligence, the legal adequacy of these injuries will likely be raised in two major contexts apart from the prima facie tort itself. First, in federal courts the lawsuit must pass the subject matter jurisdiction hurdle by showing that the data insecurity injury is sufficient for Article III standing purposes, which requires a concrete and particularized injury.[340] The second challenge to negligence claims is the economic loss rule, whereby most jurisdictions will not allow negligence claims where the injury is based solely on economic loss.[341]

1. Standing

Standing is the first hurdle that data breach suits must overcome.[342] Standing is based on the separation of powers, with the goal of ensuring that court resources are allocated to cases where the plaintiff has a personal stake in the outcome.[343] To establish standing, a plaintiff has to establish an injury-in-fact that is "concrete, particularized, and actual or imminent."[344] In standing jurisprudence, an injury-in-fact is "an invasion of a legally protected interest."[345]

In 2013, the Supreme Court decided *Clapper v. Amnesty International*.[346] The case concerned whether Amnesty International had standing to challenge the constitutionality of warrantless surveillance. In a 5-4 decision, the Court held that the possible future harm of warrantless surveillance was too speculative for the injury to be "certainly impending."[347] Amnesty International had made costly changes to protect their communications against surveillance, but the Court rejected that theory of injury as well, stating that "respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[348] The main contribution of *Clap-*

337. Solove & Citron, *supra* note 27, at 754.
338. *Id.* at 755.
339. Richards & Solove, *supra* note 145, at 1922.
340. *E.g.*, Martecchini, *supra* note 20, at 1475.
341. *Id.* at 1491.
342. Solove & Citron, *supra* note 27, at 739.
343. Cave, *supra* note 113, at 770–71; Martecchini, *supra* note 20, at 1475–76.
344. Clapper v. Amnesty Int'l, 568 U.S. 398, 409 (2013); Cave, *supra* note 113, at 772, 787.
345. Martecchini, *supra* note 20, at 1475.
346. 568 U.S. at 398.
347. *Id.* at 401.
348. *Id.* at 402.

per for standing jurisprudence was its invalidation of the use of an "objectively reasonable likelihood" standard for standing based on the risk of future harm.[349]

Because of its reliance on information injuries, *Clapper* is fairly easy to analogize as a sibling of data breach cases.[350] Some courts have used *Clapper* to support a finding that data breach plaintiffs do not have standing.[351] This is flawed reasoning because the information collection was itself speculative in *Clapper*.[352] Plaintiffs had no way of knowing if the government was surveilling their communications because that information was classified.[353] Data breach cases, on the other hand, typically involve known unauthorized information collection, at least when the theft is electronic. The speculative question just concerns when or if that information will be used unlawfully.[354]

Clapper would be more directly analogous to data breach cases if the surveillance had been known, but its use against the target was speculative. In the alternative, a dismissal that relies on *Clapper* would be reasonable if the plaintiff sued on the theory that a company they entrust with their data *might* experience a data breach. Otherwise, using *Clapper* to justify the dismissal of data breach claims based on known unauthorized collection is comparing apples to oranges.

Beck v. McDonald is a Fourth Circuit data breach standing case brought after the theft of four boxes of pathology reports and a laptop containing unencrypted patient files.[355] The court did not find a substantial risk of identity theft harm, so they rejected the argument that the theft was enough for standing.[356] One of the reasons that the court did not find standing was that such a finding would require too many assumptions, like that the laptop was stolen for the information contained within it.[357]

Other than the Fourth Circuit, the Third Circuit is the only other federal appellate court so far to deny that data breach plaintiffs have suffered injuries sufficient for standing purposes.[358] Several district courts have ruled against standing in data breach cases.[359] In *Katz v. Pershing*, the First Circuit declined to find standing for a plaintiff who learned that their nonpublic personal information was not being stored securely.[360] But, in so holding, the *Katz* court

349. Martecchini, *supra* note 20, at 1480.

350. Wooten, *supra* note 113, at 233–34.

351. *E.g., In re* Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014).

352. *Clapper*, 568 U.S. at 401.

353. *See* Wikimedia Found. v. Nat'l Sec. Agency, 857 F.3d 193, 210 (4th Cir. 2017) ("Because details about the collection process remain classified, Wikimedia can't precisely describe the technical means that the NSA employs."); Solove & Citron, *supra* note 27, at 740 n.19.

354. Cave, *supra* note 113, at 774.

355. 848 F.3d 262 (4th Cir. 2017).

356. *Id.* at 272.

357. *Id.* at 275.

358. Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011).

359. *See generally* Peters v. St. Joseph Serv. Corp., 74 F. Supp. 3d 847 (S.D. Tex. 2015); *In re* SAIC, 45 F. Supp. 3d 14 (D.D.C. 2014).

360. 672 F.3d 64, 69 (1st Cir. 2012).

pointed out that the plaintiff in the instant case was distinguishable from plaintiffs in cases of confirmed data theft.[361]

Furthermore, the Third Circuit later found standing in a data breach case based on a violation of the Fair Credit Reporting Act ("FCRA").[362] In the *Horizon* case, the Third Circuit focused on the nature of the law and stated that "when it comes to laws that protect privacy, a focus on economic loss is misplaced."[363] Thus, in the Third Circuit, a party likely will not have standing if there is no identifiable injury like actual identity theft,[364] but if the defendant violated a privacy statute by failing to prevent a breach, that might be sufficient for standing even absent economic loss.

While some courts have used *Clapper* when dismissing data breach claims for lack of standing, there are other courts that have ruled the other way. In *Galaria v. Nationwide Mutual Insurance Company*, the Sixth Circuit found that data breach plaintiffs had alleged a substantial risk of future harm sufficient for standing.[365] Likewise, the Seventh Circuit found in two cases that data breaches can cause injuries for the purposes of standing.[366] Like *Galaria*, in *Remijas*, the Seventh Circuit concluded that there was a substantial risk of future harm.[367] The Eighth Circuit in *In re Supervalu*, on the other hand, did not find substantial risk of future identity theft harms but still found that data breach plaintiffs had standing based on a present injury.[368] In *Galaria*, the breached defendant was an insurance company, and the compromised information included names, birthdates, social security numbers, and driver's license numbers.[369] *Remijas, Lewert,* and *In re Supervalu* were limited to payment card information.

These three circuits take similar but differing approaches to data breach harms. There are also several parallels between the cases. In *Galaria*, one of the named plaintiffs uncovered attempts to open credit card accounts in his name.[370] In *Remijas*, owners of 9,200 of the compromised credit cards experienced fraudulent charges.[371] In both *Lewert* and *In re Supervalu*, one plaintiff experienced fraudulent charges and other plaintiffs paid for measures like credit monitoring services.[372] The Sixth Circuit in *Galaria* did not draw a clear line

361. *Katz*, 672 F.3d at 80 (citing Anderson v. Hannaford Bros., 659 F.3d 151, 164–65 (1st Cir. 2011)).

362. *In re* Horizon Healthcare Serv. Inc. Data Breach Litig., 846 F.3d 625, 636 (3d Cir. 2017).

363. *Id.*

364. Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (finding no standing in case where claims alleged violations of the New Jersey Identity Theft Protection Act and the New Jersey Consumer Fraud Act); Complaint at 10, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (No. 2:10-cv-05142), 2010 WL 11199509.

365. 663 F. App'x 384, 388 (6th Cir. 2016).

366. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 969 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015).

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

368. *In re* SuperValu, Inc., 870 F.3d 763, 774 (8th Cir. 2017).

369. *Galaria*, 663 F. App'x at 386.

370. *Id.* at 387.

371. *Remijas*, 794 F.3d at 692.

372. *In re SuperValu Inc.*, 870 F.3d at 767; Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965 (7th Cir. 2016).

between present and future injuries for standing purposes, but the Seventh and Eighth Circuits did.[373]

There is also disagreement on whether paying for services to protect against identity theft counts as a present injury. In both *Remijas* and *Lewert*, the Seventh Circuit concluded that mitigation costs to prevent identity theft were present injuries.[374] But, the Eighth Circuit in *In re Supervalu* found the risk of future identity theft to be too speculative, and thus mitigation costs for preventing that future injury were not sufficient for standing purposes.[375] The *Supervalu* plaintiff whose compromised credit card had been used fraudulently, on the other hand, had present standing.[376] All three of these cases operate under the assumption that the injury from a data breach is identity theft. If data injuries were recognized as existing immediately when there is a data breach, it would take the data breach standing analysis out of the thorny area of standing for future injuries.

Remijas and *Lewert* are two of the most recent Seventh Circuit decisions on the topic, but an older Seventh Circuit case likewise found standing. In *Pisciotta v. Old National Bancorp*, the court ruled that the plaintiffs had standing based on the risk of future harm even though there was no indication of data misuse.[377] Commentary is divided over whether *Clapper* overruled that aspect of *Pisciotta*.[378]

The Ninth Circuit has not revisited data breach standing since *Clapper*. In a pre-*Clapper* decision, though, the Ninth Circuit found that the theft of a laptop created an increased risk of future identity theft sufficient for standing.[379] Thus, fear of future injury may be enough to clear the standing hurdle in some jurisdictions. Without something more, though, claims are likely to be dismissed because state law does not recognize that injury as compensable.[380]

One possible way to establish an injury for standing purposes, at least in some jurisdictions, is to show that the defendant's conduct violated a right established by statute.[381] Data breach cases after *Clapper* often emphasize similar factors to establish imminence for standing purposes, including the data thief's intentions, the defendant's methods for protecting the data, and whether there has been an "attempted misuse of the stolen data."[382]

373. *Galaria,* 663 F. App'x at 391; *See Lewert*, 819 F.3d at 966–67; *In re SuperValu Inc.*, 870 F.3d at 769, 774.

374. *Lewert*, 819 F.3d at 967; *Remijas*, 794 F.3d at 694 ("In addition to the alleged future injuries, the plaintiffs assert that they have already lost time and money protecting themselves against future identity theft and fraudulent charges.").

375. *In re SuperValu, Inc.*, 870 F.3d at 771.

376. *Id.* at 773.

377. 499 F.3d 629, 634 (7th Cir. 2007).

378. *E.g.*, Martecchini, *supra* note 20, at 1483–86 (noting different interpretations by courts).

379. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

380. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 282 (S.D.N.Y. 2008); Cave, *supra* note 113, at 769; Martecchini, *supra* note 20, at 1491.

381. Wooten, *supra* note 113, at 240.

382. Martecchini, *supra* note 20, at 1493.

The statutory injury approach was the next aspect of standing considered by the post-*Clapper* Supreme Court. Shortly after *Clapper*, the Supreme Court revisited standing in *Spokeo v. Robins*.[383] *Spokeo* was about standing based on the defendant's violation of the FCRA.[384] In *Spokeo*, the plaintiff sued a personal data aggregating company for displaying false information about him.[385] The Court concluded that there was no harm alleged in this false posting.[386]

A year later, the Third Circuit applied *Spokeo* to a data breach case and found harm sufficient for standing.[387] The *Horizon* litigation was based on the FCRA, just like the *Spokeo* litigation, but the Third Circuit based its decision on precedent that economic loss is not the proper measure of harm for standing purposes when standing is based on a violation of a privacy law.[388] The Third Circuit thus implicitly concluded that the *Spokeo* plaintiff had not experienced any kind of loss from the posting of false information, economic or otherwise.[389] Those affected by the *Horizon* data breach, on the other hand, had their privacy violated because true information was disseminated.[390] The implications of the Third Circuit's post-*Spokeo* decision should be the focus of future research. *Horizon* reinforces the dichotomy of privacy and defamation where the latter is the realm of false information and the former is the realm of truth, but it also leaves the false light tort in an awkward place.

The general rule forming from standing cases appears to be a preference for finding standing when there has at least been one incident of attempted fraud, whether that was a fraudulent credit card charge or a failed attempt to open a new credit account in the victim's name.[391] The clearest way to reduce standing ambiguity would be to enact a statute that establishes a consumer right to have their personal information protected. Such a statute would also formalize a duty to secure data.

2. Economic Loss Rule

Another challenge for negligence claims is the economic loss rule, which limits recovery for purely economic losses with no corresponding physical injury.[392] Generally speaking, defendants do not have a duty to protect others from economic losses. In the Oregon case of *Paul v. Providence Health System-Oregon*, however, the court noted that "[d]amages for purely economic losses . . . are available when a defendant has a duty to guard against the economic

383. Solove & Citron, *supra* note 27, at 743.
384. *Id.*
385. *Id.*
386. Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1550 (2016).
387. *In re* Horizon Healthcare Serv. Inc. Data Breach Litig., 846 F.3d 625, 636–37 (3d Cir. 2017).
388. *Id.* (quoting *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 272–74 (3d Cir. 2016)).
389. *Id.* at 638.
390. *Id.* at 640.
391. Solove & Citron, *supra* note 27, at 750.
392. Cave, *supra* note 113, at 785–86; Johnson, *supra* note 141, at 26; Martecchini, *supra* note 20, at 1491; Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1580; Simpson, *supra* note 3, at 686; Wooten, *supra* note 113, at 232.

loss that occurred."[393] This duty, according to the *Paul* court, can arise due to relationships or statutes.[394] The *Paul* court's analysis of the risk of future harm from a data breach echoes breach cases about standing: in the absence of present damages, plaintiff could not establish claims for credit monitoring damage.[395]

The economic loss rule serves to avoid excessively broad liability rulings, provide certainty for damages issues, and reinforce the occasionally porous border between the legal realms of contracts and torts.[396] Some states have exceptions to the economic loss rule.[397] The New Jersey Supreme Court held:

> [A] defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury, to particular plaintiffs or plaintiffs comprising an identifiable class with respect to whom defendant knows or has reason to know are likely to suffer such damages from its conduct.[398]

The court emphasizes that being in an "identifiable class" requires more than mere foreseeability—it must be "particularly foreseeable."[399] As other cases about duties in negligence law have shown, simple foreseeability is generally sufficient to establish a duty to a plaintiff who has suffered personal or property damage.[400] The economic loss rule is thus basically a rule about duty based on the category of the injury.

Of course, the economic loss rule relies on a dichotomy of economic harm and physical harm. To the extent that courts begin to distinguish data injuries from economic harm, the economic loss rule may prove to be inapplicable. We characterize data injuries as privacy injuries that can weaken autonomy, which would probably not trigger the economic loss rule.

3. Privacy, Identity, and Autonomy

Privacy is often characterized as a negative freedom, in that it provides a freedom *from* something instead of a power to take a specific action.[401] Rights theorists often characterize a freedom from something as an immunity.[402] The interest which is protected by an immunity is an interest that others do not have the power to violate.[403] Thomson identifies the rights of privacy and liberty as

393. 273 P.3d 106, 110 (Or. 2012).
394. *Id.*
395. *Id.* at 111.
396. Johnson, *supra* note 141, at 26–27.
397. *Id.* at 28.
398. People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985).
399. *Id.* at 116.
400. *E.g.*, Palsgraf v. Long Island R.R. Co., 162 N.E. 99 (N.Y. 1928).
401. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 748 (1999).
402. *E.g.*, JUDITH JARVIS THOMSON, THE REALM OF RIGHTS 282 (1990).
403. *Id.* at 283 ("To say that X has a certain immunity against Y is to say that Y lacks the power to make the relevant alterations in X's rights.").

both being "cluster rights" where different aspects of the right overlap with other rights.[404]

This plays out frequently in privacy scholarship, where the question is often framed as a tension between privacy and free speech.[405] To what extent can *A* be limited in his power to talk about *B*? In *New York Times v. Sullivan*, the Supreme Court held that restrictions on speech imposed by tort law were subject to constitutional restraints.[406] *Sullivan* was a defamation case, but the Supreme Court later expanded its reasoning to the false light tort.[407] Richards and Solove note that modern courts tend to view privacy law as being in conflict with the First Amendment in part due to Prosser's approach to privacy law, discussed below.[408] The truth may actually be that First Amendment complications are not the same across all information privacy issues and that some targets, like databases, hardly implicate the First Amendment at all.[409]

This Article is primarily focused on data breaches and data misuse. Data misuse may occur when companies entrusted with customer information use "that information for unauthorized commercial or other purposes."[410] One example is the recent controversy surrounding ChoicePoint, a company that inadvertently sold personal information of 163,000 people to identity thieves posing as legitimate businesses.[411] Of the people whose information was sold, at least 800 people were subsequently victims of identity theft.[412] Another example of data misuse is the controversy involving Facebook and Cambridge Analytica, where the latter is alleged to have misused the Facebook data of 87 million people.[413]

a. The Evolution of Privacy Theory and Privacy Law

The value of privacy is sometimes disputed. Is privacy even a desirable condition? Is privacy essential within a certain set of values? Philosophers have been trying to get a grasp on the nature of goodness for as long as there have been philosophers. One theory of personal morality separates goodness into

404. *Id.* at 285.

405. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 385 (1960); *see also* Ludington, *supra* note 62, at 162–63 (noting the decline of the public disclosure of private facts tort due to its conflict with the First Amendment when communications when there is a public interest in that information being known); Richards & Solove, *supra* note 145, at 1892. Prosser also expressed concern that the false light and disclosure of private facts torts involved an examination of reputation, overlapping with defamation law. Prosser, *supra*, at 398.

406. Richards & Solove, *supra* note 145, at 1902.

407. Time Inc. v. Hill, 385 U.S. 374 (1967).

408. Richards & Solove, *supra* note 145, at 1923.

409. *Id.* (arguing that database cases raise fewer First Amendment issues than tort actions about emotional injuries caused by actions of the press).

410. Rabin, *Data*, *supra* note 129, at 317.

411. *Id.*

412. *Id.*

413. Taylor Hatmaker, *Facebook's Latest Privacy Debacle Stirs Up More Regulatory Interest from Lawmakers*, TECHCRUNCH (Mar. 17, 2018, 8:40 PM), https://techcrunch.com/2018/03/17/facebook-cambridge-analytica-regulation-klobuchar-warner/.

two categories: intrinsic goodness and instrumental goodness.[414] Instrumentally good things are said to be so because these things are effective for achieving intrinsic goodness.[415] Privacy would likely not be considered intrinsically good, but in a society that strongly values individuality, privacy has instrumental goodness because it allows an individual to limit their exposure to the public, thus empowering stronger individuality. In *Pavesich v. New England Life Insurance*, the Supreme Court of Georgia identified privacy as being derived from the "absolute rights" of personal security and personal liberty.[416]

In the United States, the legal concept of privacy evolved out of commentary and case law. In 1890, Warren and Brandeis published their seminal work on privacy, in which they focused on the "right to be let alone."[417] A key component of this right is the extent to which an individual's thoughts and other private details should be communicated to others.[418] Warren and Brandeis were moved to write this article in part due to societal and technological changes, especially the portable cameras and advances in printing technologies that allowed journalists to document the lives of noteworthy members of society.[419]

After *The Right to Privacy* was published, a common scenario in privacy case law involved a company putting a person's likeness on their packaging or in their advertisements without obtaining the person's consent.[420] These cases have been coming up again recently, as in the lawsuit against Facebook over its now-discontinued Sponsored Stories feature.[421] Through this feature, Facebook might pair a company's ads with a photo of one of the viewer's Facebook friends who had "liked" the company on Facebook. For example, if Mark clicked the "like" button on Pizza Hut's Facebook page, Mark's Facebook friend Richard might see a Pizza Hut ad that includes Mark's photo.

In 1960, Prosser published *Privacy*, which established the foundation for the major privacy torts that courts recognize today.[422] Oldberg points out that Prosser's concept of the right to privacy emphasized conduct and injuries related to privacy invasions, instead of "the overarching purpose of the right of privacy" as emphasized by Warren and Brandeis.[423] Prosser's four privacy torts are (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false

414. F.S.C. Northrop, *Law, Language and Morals*, 71 YALE L.J. 1017, 1023–24 (1962).

415. *Id.*

416. 50 S.E. 68, 70 (Ga. 1905); Jonathan Kahn, *Biotechnology and the Legal Constitution of the Self: Managing Identity in Science, the Market, and Society*, 51 HASTINGS L.J. 909, 915 (2000).

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

418. Oldberg, *supra* note 48, at 197–98.

419. Gasser, *supra* note 144, at 62.

420. *E.g.*, *Pavesich*, 50 S.E. at 69 (concerning an advertisement with customer testimonial next to plaintiff's likeness, where statement was not made by plaintiff and plaintiff had not consented to the use of his image).

421. Brian Feldman, *Facebook Reaches Settlement in Sponsored Stories Lawsuit*, ATLANTIC (Aug. 27, 2013), https://www.theatlantic.com/technology/archive/2013/08/facebook-reaches-settlement-sponsored-stories/311753/.

422. Prosser, *supra* note 405.

423. Oldberg, *supra* note 48, at 198.

light publicity, and (4) appropriation of identity.[424] Several scholars have observed that Prosser's four privacy torts have questionable utility for modern problems.[425] Some have criticized these torts as being too narrow and rigid.[426] This was likely by design, as Prosser harshly criticized the ways that privacy law was "expanded by slow degrees to invade, overlap, and encroach upon a number of other fields."[427]

Ludington asserts that applying existing privacy torts to information misuse is like "suggesting that one could use a toy drill to fix a nuclear reactor."[428] Richards and Solove say that the general consensus is that privacy tort law is ineffective to address issues in the Information Age.[429] There are many reasons why Prosser's privacy torts are viewed as inadequate for addressing data insecurity injuries. The invasion of privacy tort, for example, requires a publication that may not be present if data was simply stolen and not posted elsewhere.[430] Even if the data is published elsewhere, it was likely not "published" by the company whose systems were breached. Intrusion upon seclusion would not be an appropriate claim in most data breach cases because the defendant was not the one to invade the customer's privacy interests.[431] Rather, that invasion was by a third party. Similarly, the false light tort will generally be inapplicable to data breaches involving truthful information.[432]

To more adequately address digital harms, some commentary has suggested a return to the Warren and Brandeis approach to privacy that focuses more on autonomy and the individual's right to decide how they are portrayed to the world.[433] Autonomy is often a focus in case law related to an individual's private decisions.[434] Boone defines autonomy as "an individual's ability to make choices about his or her own experience and identity, as well as the process of effectuating those choices."[435] Ludington describes the harm caused by information misuse as an injury to autonomy.[436] Data insecurity injuries cannot really be categorized as economic injuries or physical injuries, but such injuries do interfere with the ability to have control over one's personal information. In this sense, a data insecurity injury, whether caused by data breach or data misuse, is an injury to autonomy.

424. Prosser, *supra* note 405, at 389.

425. Danielle Keates Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1807 (2010); Richards & Solove, *supra* note 145, at 1887.

426. Richards & Solove, *supra* note 145, at 1890.

427. Prosser, *supra* note 405, at 422.

428. Ludington, *supra* note 62, at 159.

429. Richards & Solove, *supra* note 145, at 1889.

430. Wooten, *supra* note 113, at 231–32. It should be noted, however, that the Fourth Circuit recently found that the exposure of patient files was a publication for purposes of insurance coverage for a data breach. *See* Travelers Indem. Co. of Am. v. Portal Healthcare Sol., LLC, 644 F. App'x 245, 247–48 (4th Cir. 2016).

431. Ludington, *supra* note 62, at 160.

432. *Id.* at 166.

433. Oldberg, *supra* note 48, at 203.

434. Meghan Boone, *The Autonomy Hierarchy*, 22 TEX. J. ON C.L. & C.R. 1, 15 (2016) (discussing the ways that courts treat spiritual autonomy and physical autonomy).

435. *Id.* at 16.

436. Ludington, *supra* note 62, at 147.

Informational privacy is a category of privacy that has become more important in a networked world. Alan Westin, an early information privacy scholar, defined this type of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[437]

Privacy law has historically evolved alongside technological developments.[438] Gasser expresses concern that the legal dimension of information privacy is not sufficiently engaged with the technical dimension.[439] Perhaps that is because it is not really technology that pushes privacy law forward, but marketing. With improvements in photographic technology, random photos were used to sell products. With improvements in data analytics and web programming technology, photos of the target's friends are used to sell products. Both innovations raised privacy concerns for people who did not consent to this use of their image for someone else's commercial benefit.

The increasing interest in the data analysis activities of Cambridge Analytica raises another opportunity for privacy law to develop in response to the use of personal information that causes discomfort. Cambridge Analytica describes itself as specializing in psychographic voter data, and one of the ways that it developed its business initially was by scraping 50 million Facebook profiles.[440] Facebook learned of the activity in 2015 and allegedly asked Cambridge Analytica to stop.[441] Cambridge Analytica became the subject of international controversies after their data analysis practices were revealed as having been applied in the promotion of misleading stories and political ads during the 2016 presidential election in the United States.[442] The FTC has announced a probe of Facebook's data practices.[443]

It is fair to say that privacy law evolves when technology enables a new and uncomfortable use of personal information. How should the law respond to significant technological changes? Gasser identifies three common response patterns in this context: (1) subsumption, where the legal system tries to apply the old rules to new problems; (2) gradual innovation and incremental changes; and (3) more radical suggestions for transforming legal approaches.[444] A subsumption approach to data insecurity injuries would probably require accepting an analogy that allows existing law to easily be adapted to the new technological environment.[445] Data breach notification laws are an example of gradual innovation because such laws focus on notification rather than prevention. Notification laws are useful for building context while working towards a larger

437. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1970).

438. Gasser, *supra* note 144, at 63.

439. *Id.* at 67.

440. Cadwalladr & Graham-Harrison, *supra* note 68.

441. *Id.*

442. *Id.*

443. Sara Salinas, *Facebook Stock Slides After FTC Launches Probe of Data Scandal*, CNBC (Mar. 26, 2018), https://www.cnbc.com/2018/03/26/ftc-confirms-facebook-data-breach-investigation.html.

444. Gasser, *supra* note 144, at 64.

445. *Id.*

goal, but their utility is limited. A more radical suggestion might involve the creation of a new administrative agency to track and manage data insecurity issues.

Personal information is a vital component of a person's identity. You can tell a lot about a person given unlimited information about where they go, what they do, and what they like. These items of information have also become part of a very popular business model driven by customer data. Such businesses take information that was of no independent value to the person and then include that information in a large database of similar consumers. In effect, they mined the raw material of identity and made it a commodity. There are legitimate businesses that do this, often called data traders, but there is also a black market for more specific data like credit card and social security numbers.[446] Following a data breach, stolen information may pop up in this black market. In the grey area where people are uncomfortable but pretty sure that it's still legal, there are companies like Cambridge Analytica.

Much of the discussion about data insecurity injuries concerns economic loss. This limitation, however, is untenable because of the nature of what has been taken. No value is assigned to one's shopping habits or medical history until it is commodified by a third party. Strict adherence to Fair Information Practices could potentially mitigate some of the data insecurity issues, and that includes ensuring that individuals "have a meaningful choice about how their data is used."[447] But an economic analysis of data breach harms will end at an impasse, similar to the fate of the plaintiff in the unusual case of *Moore v. Regents of the University of California*.[448]

b. Diseased Spleens and Data Privacy

In *Moore*, the plaintiff had a diseased spleen, which was surgically removed.[449] Researchers realized that Moore's cell line was very valuable to their work. They continued using Moore's cells, occasionally collecting new samples from him, and then obtained a patent for the cell line.[450] Moore learned of the patent and sued for conversion of his property.[451] The California Supreme Court declined to expand the tort of conversion to include human cells, with the majority reasoning that such a ruling could stifle scientific research.[452] Judge Arabian, concurring, focused instead on the moral implications of allowing someone "to sell one's own body tissue *for profit*."[453] In a dissent, Judge Mosk was similarly offended, but his offense was directed more towards the gall of

446. *Id.*; Ludington, *supra* note 62, at 184.
447. Ludington, *supra* note 62, at 185.
448. 793 P.2d 479, 496 (Cal. 1990).
449. *Id.* at 485.
450. *Id.* at 481, 511.
451. *Id.* at 487.
452. *Id.* at 494.
453. *Id.* at 497 (Arabian, J., concurring) (emphasis in original).

using someone else's body tissue for profit without the subject's consent.[454] Moore's cells, this constitutive element of his identity, thus looked very different to Arabian and Mosk. Arabian criticized the plaintiff for wanting to profit off of the use of his cells, and Mosk criticized the defendant for profiting from Moore's cells without his knowledge or consent.

Mosk also dissented in a later case with similar themes. In *Intel Corp. v. Hamidi*, the majority concluded that sending mass emails to Intel's employees was not, by itself, enough to show an injury for purposes of a conversion claim.[455] In *Hamidi*, Mosk's dissent asserted that the act of sending mass emails to Intel's servers constituted misappropriation.[456] Mosk's dissents represent a property-based concept of intangible harms to both identity and network resources.

Moore's cells make up part of his identity because they represent a constitutive element of the self. Personal information, likewise, can enable someone to recreate an identity. Consider Jane, a thirty-five-year-old single mother who makes frequent trips between New York City and Atlanta. The various data points that marketers have for her enable targeted advertising. Advertisers would likely assume that Jane will be more frugal as a single mother. Perhaps when she is in Atlanta in the winter, Jane would be responsive to ads for end-of-season sweater sales. If the advertisers come to this conclusion, Jane might find that as soon as she lands in Atlanta in February, she starts receiving advertisements about a clearance sale at Bloomingdale's.

The companies that collect the data and sell it for marketing purposes have taken a raw ingredient, like Moore's cell line, and combined it with other ingredients to create a product. If Jane sues a company that has monetized her information, what should be the outcome? Using the majority's reasoning in *Moore*, would it put an important interest at risk to allow consumers to share in the profits from monetization of their personal information? Or is there a moral argument as in Arabian's concurrence?

Rojas-Lozano v. Google Inc. offers an appropriate big data analogy to *Moore*.[457] That case concerned Google's practice of using its reCAPTCHA tool to have their customers recognize characters for the digitization of books.[458] In *Rojas-Lozano*, Google took a tiny thing from a lot of people, that being their time, and turned that into something of value for themselves.[459] Google's newer reCAPTCHA system often requires the identification of street signs, so it is possible that the process is now being used to improve the artificial intelligence of self-driving cars.[460]

454. *Id.* at 508–09 (Mosk, J., dissenting); Kahn, *supra* note 416, at 933–34.
455. 71 P.3d 296, 311 (Cal. 2003).
456. *Id.* at 325–26 (Mosk, J., dissenting).
457. 159 F. Supp. 3d 1101 (N.D. Cal. 2016).
458. *Id.* at 1107.
459. *Id.*
460. *See, e.g.*, *Self Driving*, XKCD, https://xkcd.com/1897/ (last visited Nov. 2, 2018).

Privacy and autonomy were both in issue in the *Moore* case.[461] These concepts were also important in *Pavesich v. New England Life Insurance*, where the court ruled that the plaintiff was deprived of control over his identity when the defendant used his image to promote their product without his consent.[462] The *Pavesich* court adopts a broad definition of liberty, stating that the word "means the right not only of freedom from servitude, imprisonment, or restraint, but the right of one to use his faculties in all lawful ways, to live and work where he will, to earn his livelihood in any lawful calling, and to pursue any lawful trade or avocation."[463]

In *Moore*, the judges and courts vacillated between being appalled that Moore wanted property rights in his own cells and being appalled that the researchers wanted property rights in Moore's cells. Kahn saw a slippery slope between property rights in someone's cells and property rights in someone's identity.[464] By commodifying identity in general, Kahn warned, the market threatens individual identity.[465]

Moore's ignorance of the use of his cells also makes the *Moore* case one about informed consent and deception.[466] Normally, harms caused by deception and fraud are measured as economic injuries, but perhaps it would be more appropriate to view deception as a harm to dignity because deception interferes with a person's ability to make decisions based on full and accurate knowledge. After all, lies affect how the recipient interacts with the world and taint their decision-making process.

c. Privacy Torts

The Internet has given rise to new media, and the privacy torts were not designed to deal with the sort of issues posed by social networking and bloggers.[467] Most modern discussion of privacy torts relies on Prosser's formulations. Richards and Solove note that modern privacy tort cases are difficult to win for plaintiffs.[468] As discussed above, the four main privacy torts in the United States are (1) intrusion upon seclusion, (2) appropriation of identity, (3) public disclosure of private facts, and (4) false light. If digital data injuries can be identified with one of the privacy torts, they become privacy injuries, which courts are more familiar with. That way, the question of whether an injury exists for negligence purposes is simplified. Unfortunately, this juxtaposition proves to be a tall order.

461. *See generally* Moore v. Regents of University of California, 793 P.2d 479 (Cal. 1990).

462. 50 S.E. 68, 80 (Ga. 1905); Kahn, *supra* note 416, at 916.

463. *Pavesich*, 50 S.E. at 70.

464. Kahn, *supra* note 416, at 935, 938 ("Granting legal recognition to the constitutive elements of identity is a logical corollary of recognizing its outward manifestations in names or images.").

465. *Id.* at 951.

466. *Id.* at 910 (arguing that ensuring informed consent does not protect personal identity).

467. Richards & Solove, *supra* note 145, at 1919.

468. *Id.* at 1918.

Intrusion upon seclusion claims require a subjective and objective analysis of the plaintiff's expectation of privacy.[469] Prosser referenced an intrusion upon seclusion case that predated Warren and Brandeis's article.[470] In *De May v. Roberts*, a patient sued her doctor for bringing a nonprofessional companion to her home while she was giving birth.[471] The doctor had asked a friend to accompany him on the visit and did not inform the patient or her husband that the friend was neither a doctor nor a medical student.[472] Instead, he simply explained that the young man was there to carry his things, and the patient presumed that the doctor's relationship with the man was a professional one.[473] She was mortified to learn that a stranger with no medical background was present for the birth of her child.[474] The court in turn was appalled at this intrusion into a sacred occasion in this woman's life and allowed her to recover damages.[475] A modern day analogy in the big data context might be a customer learning that their private medical information was shared with a marketing firm without their consent. There thus may be some potential for the intrusion upon seclusion tort in cases of data misuse like the actions of Cambridge Analytica. Most data breach incidents, however, would not fit within a similar fact pattern. It is also unclear how far the intrusion upon seclusion analogy could go for data misuse. In the Cambridge Analytica and Facebook controversy, the data misuse concerned the aggregation of information disclosed to each person's 400 closest friends.[476] Even a friends-only Facebook post may still have too wide of an audience to truly be considered "seclusion."

The appropriation of identity tort typically involves the use of "another's name or likeness for commercial gain."[477] The plaintiff is generally not a celebrity in those cases, contrasting the appropriation tort against the right of publicity where the plaintiff is often already famous.[478] Kahn analyzed the implications for the philosophical concept of the self that can be derived from one of the lower court decisions in *Moore v. Regents of the University of California*.[479] Kahn cast the central dispute in *Moore* as one of appropriation of identity, tying genetic information to one's identity in the same way as one's likeness.[480] This

469. Ludington, *supra* note 62, at 161.

470. Prosser, *supra* note 405, at 389.

471. 9 N.W. 146, 146 (Mich. 1881).

472. *Id.* at 147.

473. *Id.*

474. *Id.*

475. *Id.* at 165–66. It should be noted that Prosser's conclusion in *Privacy* lacked some internal consistency. Prosser wrote that "by the use of a single word supplied by Warren and Brandeis, the courts have created an independent basis of liability, which is a complex of four distinct and only loosely related torts . . . ." Prosser, *supra* note 405, at 422. The 1881 case of *De May v. Roberts*, however, explicitly referred to the plaintiff's "legal right to the privacy of her apartment." 9 N.W. 146, 149 (1881). The court could not have been referring to a constitutional right of privacy, because neither Dr. De May nor Mr. Scattergood were government actors. Prosser does not address how this dignitary harm fits into his proprietary model.

476. Cadwalladr & Graham-Harrison, *supra* note 68.

477. Kahn, *supra* note 416, at 915.

478. *Id.* at 917; Ludington, *supra* note 62, at 167.

479. Kahn, *supra* note 416, at 914.

480. *Id.* at 950.

is in line with Prosser's view of the appropriation tort as a proprietary injury instead of a mental injury,[481] and contrary to Warren and Brandeis' vision of privacy injuries as "injury to the feelings" that interfere with "a person's ability to develop her 'inviolate' personality."[482]

The tort of appropriation is an option for some data breach cases because it is based on a harm to dignity caused by denying the right to control one's personal information.[483] As an intentional tort, though, appropriation claims would be stronger against the data thief in data breach cases. An appropriation claim might be a strong cause of action against Dr. Kogan, the researcher who sold data about Facebook users to Cambridge Analytica.

In an appropriation of identity case, damages are awarded with the goal of "vindicating and rehabilitating the subject's dignity."[484] In *Moore*, the appellate court recognized a dignitary interest for Moore, though it still couched the interest in proprietary terms.[485] Kahn suggests that the majority in *Moore* should have acknowledged that the use of Moore's cells without his consent amounted to a dignitary harm.[486] This, of course, was not what Moore wanted. Moore had argued for a property interest because a successful claim would yield much higher damages than a simple injury to dignity.[487] But, that is an issue of remedy, and if a data breach can be shown to have caused a dignitary injury, that should satisfy the injury requirement.

A data breach case involving a release of personal information might be addressed with the public disclosure of private facts tort, though again, as an intentional tort, negligent actions may not be enough. Additionally, for the public disclosure of private facts tort, the disclosure must generally be of an embarrassing nature.[488] This creates a problem with many modern information privacy injuries because a lot of information collection is largely innocuous.[489] In *Shibley v. Time, Inc.*, the magazine's sale of subscriber information to advertisers was found to not meet the requirements of causing "mental suffering, shame or humiliation to a person of ordinary sensibilities."[490]

The tort of negligent infliction of emotional distress, while not a privacy tort, is also a possible guide for data injuries stemming from security breaches. Specifically, plaintiffs in some jurisdictions can recover for negligent infliction of emotional distress claims if they were within the zone of danger.[491] Expanding the zone of danger rule to data insecurity injuries, however, might result in overbroad enforcement. Should someone be considered to be in the zone of

481. Richards & Solove, *supra* note 145, at 1916.
482. Solove & Citron, *supra* note 27, at 768–69.
483. Kahn, *supra* note 416, at 922.
484. *Id.* at 917.
485. *Id.* at 921.
486. *Id.* at 932.
487. *See id.*
488. Ludington, *supra* note 62, at 162.
489. Richards & Solove, *supra* note 145, at 1919.
490. *Id.*
491. Fox & Stein, *supra* note 27, at 990–91; Goldberg, *supra* note 137, at 820–21.

danger if their data is compromised? Or only after a fraud attempt has been made against at least one person whose data was leaked? Solove and Citron also note that negligent infliction of emotional distress claims often appear "in the context of relationships that impose independent, pre-existing duties of care."[492]

B. Remedies

Under contract law, the goal of damage awards is generally to put the plaintiff in the same position they would have been in had they never entered into the contract. Under tort law, damages are intended to compensate for an injury. A third purpose of damages is to prevent unjust enrichment by requiring the disgorgement of profits from wrongful acts.

A fourth purpose is more symbolic and is demonstrated by punitive damages. We noted in Section II.C that the legal system can be characterized as existing to prevent the power structure from becoming too imbalanced. Punitive damages may be characterized as a "manifestation of the law's concern with exercises and defaults in the use of power."[493] In modern law, however, punitive damages are often challenged, especially when the punitive damages are far higher than the damages from economic or physical loss.[494] In principle, punitive damages are issued for especially egregious conduct. The focus is not so much on making the plaintiff whole but on sending a message about the defendant's behavior.

There are some concerns that expanding liability for computer security-related negligence could potentially lead to a cascade of unlimited liability.[495] But without any liability, those with the most ability to prevent data insecurity injuries arguably lack sufficient incentive to prevent data insecurity injuries.[496] A compromise position might involve limitations on liability or caps on damages, perhaps limiting such damages to the cost of ongoing credit monitoring.[497] Johnson compares this option to the medical monitoring damages available in some states for victims of toxic exposure.[498]

How should individual data breach victims be compensated? This is a question that has appeared throughout the literature, and never with a satisfactory answer. Johnson suggests that "compensation should depend on the reasonableness of the amount spent to restore a good credit rating."[499] Ludington argues that to incentivize the protection of personal information, class actions

492. Solove & Citron, *supra* note 27, at 29.

493. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 57 (quoting MARSHAL S. SHAPO, THE DUTY TO ACT: TORT LAW, POWER AND PUBLIC POLICY xiii (1977)).

494. Rustad & Koenig, *Tort Monster*, *supra* note 100, at 62.

495. Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1583.

496. Johnson, *supra* note 141, at 22.

497. *Id.* at 29–30 (noting also that "a damages cap should not apply to cases involving egregious conduct").

498. *Id.* at 29.

499. *Id.* at 28.

must be available.[500] Riedy and Hanus, on the other hand, argue that the class action model is poorly suited to compensating plaintiffs whose data has been misused.[501] Rabin sees the benefits of both positions, noting that collective tort actions will likely be necessary, but that class actions would likely not be effective for addressing dignitary harms.[502]

Privacy and data injury harms create complications when it comes to damage awards because these injuries do not lend themselves easily to economic measures. But damage awards at the end of trial are uncommon anyway because most civil litigation settles before trial.[503] The terms of settlements are often sealed. Some settlements are motivated by public interest concerns and might result in a research fund being established. Class action litigation between a group of flight attendants and the tobacco industry resulted in a settlement that set up a research fund to study secondhand smoke.[504] Some settlements might take the form of administered compensation funds.[505]

Administered compensation funds can be based on statute, like worker's compensation, or based on contract, like insurance.[506] The National Childhood Vaccination Compensation Fund is an administered compensation fund with a goal of creating a more efficient process for vaccination injuries than individual litigation.[507] Similar motivations were behind Congress's creation of the 9/11 Victims Compensation Fund.[508] Administered compensation funds seem to be most appropriate for circumstances with unexpected harms, innocent victims, and incidents that were largely out of the defendants' control.[509]

Data breach cases involve many challenges for litigants and courts. Two important topics are whether such incidents cause injuries, and if so, how those injuries should be compensated. This requires flexibility, because information injuries are difficult to identify and quantify. This is nothing that courts have not done before. Society is changing, and the law will change with it, though perhaps at a slower pace.

V. RECOMMENDATIONS

In this Article, we have explored data breach litigation within a negligence framework. This is a topic that will continue to grow more important in the coming years. Data breaches in the United States often cost the targets millions of dollars, yet courts struggle in fitting these harms within current law.

500. Ludington, *supra* note 62, at 186.

501. Riedy & Hanus, *supra* note 28, at 37.

502. Rabin, *Data*, *supra* note 129, at 335.

503. Andrew S. Pollis, *Busting Up the Pretrial Industry*, 85 FORDHAM L. REV. 2097, 2099–2100 (2017).

504. Rabin, *Enabling Torts*, *supra* note 182, at 450; *Broin*, TOBACCO ON TRIAL, http://www.tobaccoontrial.org/?page_id=592 (last visited Nov. 2, 2018).

505. Riedy & Hanus, *supra* note 28, at 38.

506. *Id.*

507. *Id.* at 41.

508. *Id.*

509. *Id.* at 43.

Data misuse claims fare no better. Following the revelations that Facebook's data practices are more pervasive and detailed than users previously believed, the most compelling counter-argument that Facebook has been able to muster is that members consented to the terms that Facebook offered for the use of its services.[510] Under the current legal system where meaningless consent in the face of network effects is still viewed as being contractually valid, the average court in the United States is likely to side with Facebook. Still, there is a growing consensus that these kinds of data practices are, for lack of a more formal sounding legal term, pretty creepy. A push towards recognizing data protection duties and autonomy injuries, however, could stem the tide of creepiness.

A. Recognize Duty to Secure

Litigation over data security incidents is both numerous and unpredictable. This Article uses a negligence model to identify and describe the legal developments needed to create a more stable legal and business environment to confront modern injuries. The first and arguably most important part is the need to establish a duty to secure computer systems and protect consumer data.

1. Options for Finding a Duty

A duty to secure one's computer systems for others' benefit can be compared to premises liability.[511] The classic premises liability case involves a landlord's duty to protect tenants from crime, derived from the landlord's duty to secure common areas. Using a premises liability theory, a network operator would have a duty to secure the "common areas." The common areas for networks might include public-facing websites and the electronic interactions that employees have with external actors, plus some systems that are shared internally. The strongest claim based on premises liability after a data breach would probably come from a person who suffered financial loss as a result of identity theft or other fraud. This situation is not too different from the situation of being robbed in a poorly secured apartment building.

A second theory supporting a duty to secure concerns the nature of the service provided. In a bailment situation, the bailee typically has a duty to protect the property entrusted to them. Future work should examine the status of data in bailment relationships. Litigants have raised bailment claims in data breach cases, though there is not a consensus on the merits of the claim.[512] If

510. Maya Kosoff, *Zuckerberg Hits Users With the Hard Truth: You Agreed to This*, VANITY FAIR (Mar. 26, 2018, 11:01 AM), https://www.vanityfair.com/news/2018/03/zuckerberg-hits-users-with-the-hard-truth-you-agreed-to-this.

511. *See* Rustad & Koenig, *Cybercrime*, *supra* note 4, at 1570 (examining a premises liability theory for software flaws).

512. *E.g.*, *In re* Sony Gaming Networks and Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 1013–14 (S.D. Cal. 2012) (rejecting bailment argument because personal information was not personal property under California law).

there is a bailment relationship, this implies that data holders have a duty to secure data in a manner analogous to how bailees protect tangible property.

Aside from a premises liability or bailment analogy, data security duties could be imposed by legislation. One option for creating a duty by statute is to amend the Gramm-Leach-Bliley Act ("GLBA"). The GLBA currently gives "financial institutions" a statutory duty to secure customer information.[513] A simple amendment to expand this obligation to other data-driven industries could create a recognizable duty to secure.

Another tricky element of duty is how to tell whether an action breached that duty or if it was mere nonfeasance. The nature of cybersecurity blurs the line between misfeasance and nonfeasance. Nonfeasance, or inaction, is usually not a source for liability except in exceptional situations. Misfeasance requires some positive action. Is a failure to secure one's systems a passive or active behavior? Fundamentally, the answer will depend on whether security is an essential aspect of the product or an afterthought.

We argue that security is an essential aspect of maintaining a database, and as an essential aspect, there is an implied duty to provide adequate security that is incident to the practice of maintaining databases. Once a company has decided that access to information stored on its systems will be restricted to authorized users, this creates an implied duty to maintain secure systems for the benefit of individuals whose information is contained therein. Service providers created the environment. Such creation should also include providing for the security of that environment. Finding negligence thus ceases to be a matter of whether they notified customers after a data breach, but rather is connected to the conscious decision to not design for security.

2. Risk Management Requires Duty

In Section III.A, we examined the risk management process alongside the cognitive biases that interfere with each stage of the process.

Risk identification can be compromised when people do not have enough information about their situation, and thus ignore the surrounding risks (Simplification).

Risk analysis can be compromised when people underestimate the possibility of a disaster occurring (Optimism).

Risk evaluation can be compromised if people are too focused on short-term objectives unrelated to the possible future disasters (Myopia).

Risk treatment can be compromised if people do not implement risk mitigation strategies either because they are reluctant to change (Inertia), or due to a social norm that people do not treat the risk (Herding).

513. FED. TRADE COMM'N, *Gramm-Leach-Bliley Act*, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Nov. 2, 2018).

Risk review can be compromised if people forget to keep monitoring a risk after the risk has not materialized for a long time (Amnesia).

If risk management in cybersecurity is to be successful, the legal field must recognize the way that cognitive biases can undermine the process. One way of recognizing this is to establish a duty in order to properly apportion the burdens.

By imposing a legal duty to secure data, this connects legal risk and cyber risk. This risk bundle raises much stronger awareness than cyber risk alone because legal risk is often more visible to managers of an organization. If managers see the legal risks of bad security practices as an issue they need to address, they will have to deal with cyber risk as well. By tying legal risk to a more abstract, probability-based risk, legal policy can help risk managers avoid the Simplification bias as it becomes less likely that people will ignore the risk.

A legal duty to secure necessarily must be complemented by instructions for fulfilling this duty. Otherwise, how is one to know if there has been a breach of the duty? To this end, cybersecurity standards are vital. Standard development involves a lot of cyber risk analysis. For example, the contractors and subcontractors of the Department of Defense ("DoD") are required to comply with Defense Federal Acquisition Regulation Supplement ("DFARS") and implement proper risk controls under the NIST Cybersecurity Framework ("CSF").[514] The CSF covers a broad range of topics in cybersecurity. The CSF points out the common weaknesses in information systems that could easily go wrong and suggests the best practices to mitigate these risks. Cybersecurity standards, therefore, not only provide a benchmark for determining whether a duty has been violated, they also simplify the Analysis step of the risk management process.

Creating a legal duty to secure may even lead to benefits from the Myopia cognitive bias because the legal risk imposes short-term costs. Cybersecurity risk is intangible, and if protections are effective, the proof will be an absence of a disaster. A myopic organization can easily disregard such ethereal threats and benefits in favor of addressing more immediate problems. This further demonstrates the value of a risk bundle, where a more abstract risk is paired with a legal risk to incentivize action. Prior to the massive data breach of Target's systems in 2013, company security officers seemingly ignored a warning about the intrusion and also turned off the feature of their cybersecurity product that would have removed the malware.[515] One study showed that increased cybersecurity spending may reduce the cost of responding to a data breach.[516] By bundling cyber risks with more concrete legal risks, leaders will see that it is also in the organization's short-term interests to address cyber risks.

The end goal of overcoming cognitive biases with a legal duty is to bring about more cybersecurity investment. As more organizations and individuals

514. *See* Exec. Order, *supra* note 133; NIST, *supra* note 133.
515. Rabin, *Data*, *supra* note 129, at 315.
516. Riedy & Hanus, *supra* note 28, at 23.

adopt more secure practices, security will become a new social norm. At that stage, the Herding bias will start to reinforce socially positive actions instead of harmful actions, and the Inertia bias will no longer have an adverse effect because the default behavior has changed.

A legal requirement also makes sure that organizations monitor and review their cyber risks by requiring the adoption of a risk monitoring systems, such as the 'Continuous Security Monitoring' category under the CSF. A risk bundle thus reduces the dangers of Amnesia bias because compliance will require periodic reviews of cybersecurity status.

Therefore, a legal duty to secure combined with cybersecurity standards would improve cybersecurity by supporting all of the essential steps of risk management. As part of a risk bundle, a legal duty to secure can effectively mitigate the negative impacts caused by the six cognitive biases, even though it does not necessarily help people overcome them.

B. Recognize Injuries

Data injuries are a challenge for courts. The loss of control over personal data is not often treated as a "particularized injury" for standing purposes. This is partially due to the unwarranted focus on economic measurements of harm. Data injuries, however, are about privacy, self-determination, and autonomy. Courts should recognize the nature of these injuries and not limit their analysis to economic harms. In doing so, this will prevent data breach lawsuits from being derailed based on standing and the economic loss doctrine.

In the alternative, legislation could be enacted to formally recognize that individuals are injured at some point following a data breach. The point at which an injury exists might be immediately after, when there is anxiety about future identity theft. It might be more appropriate for an injury to not be acknowledged until the individual has accrued costs to monitor their credit. The Supreme Court has expressed concerns about plaintiffs manufacturing an injury by taking on these kinds of costs, but that is a legal fiction that assumes a very bored plaintiff.[517] Making purchases on the assumption that you will get a refund is not economically rational when the administrative costs of obtaining that refund will be extremely high. Still, the legislature might prefer a later triggering event, like some form of attempted fraud related to the breach.

Another possibility for recognizing data insecurity injuries might involve drawing lessons from Fourth Amendment jurisprudence. In recent cases, a "mosaic theory" of the Fourth Amendment has started to take shape. Using the mosaic theory, government actions that might violate the Fourth Amendment are analyzed as a collective whole.[518] The focus of the mosaic theory is generally on data collection, with the primary reasoning being that if a lot of tiny data collection incidents take place that would not, on their own, amount to a violation of the Fourth Amendment, they may still amount to a violation taken in the aggregate.[519]

A mosaic theory of data breach liability might assist in evaluating both breach and injury. In the breach of duty context, a mosaic theory might examine a data holder's security practices collectively, with no single practice being determinative of whether a duty to secure was breached. A mosaic theory of data insecurity injury could focus on the scope of the data breach, both in types of information and the number of records breached. A small breach of a large amount of information might be worse than a large breach of a limited type of information. Viewing the incident holistically can thus provide clear justification for recognizing that an injury exists.

517. *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 389 (6th Cir. 2016) ("This is not a case where Plaintiffs seek to 'manufacture standing by incurring costs in anticipation of non-imminent harm.' Rather, these costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the requirement of Article III standing.") (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013)).

518. Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 311 (2012).

519. *Id.* at 320.

C. Data Injury Compensation and Research Fund

Our third recommendation builds on a recommendation by Riedy and Hanus to establish a compensation fund for data breach victims, though we disagree with the authors' broad opposition to litigation. Riedy and Hanus strongly disagree with the trend towards litigation of data breaches, going so far as to imply that the "rush to the courthouse" following a data breach is an unjustified "hysterical response" to the threat.[520] In their article, the authors argue without much support that data breach notification statutes are a better deterrence for data breaches than litigation.[521]

There is, however, merit in challenging the traditional litigation model of conflict resolution, especially in response to new technologies and new injuries. In this Article, we have argued in favor of recognizing injuries and duties in data breach litigation. By adopting a mosaic theory of data injuries, for instance, courts will become better equipped to recognize the nuances of digital harms. Stealing a single line of a database is not like stealing a book from someone's house, but when that database contains millions of lines, it is hard to deny that this was a theft that resulted in some type of harm.

Individual recoveries after data theft, however, are almost always very small, so class actions are necessary to justify the administrative costs. If the costs of litigation prove to be too high, then data breach class actions will have been shown to be an inefficient method of responding to the societal injury caused by data insecurity. In such a situation, a compensation fund as a replacement for litigation would be advisable.

Yet we believe that such a fund would be more beneficial as a complement to litigation, rather than a substitute. For that reason, we suggest the creation of a Data Injury Compensation and Research Fund ("DICARF"). Joining a class action would waive a right to individual recovery from the fund, but if the class action proceeds to a settlement, class members would have the option of taking a payout or having their part of the settlement included in a payment to DICARF.

This recommendation is ultimately about improving access to justice and security. An individual payout of five dollars after a data breach may be inefficient. With millions of data breach victims, each individual could be benefited much more if the payments by breached companies went towards an investment in socially beneficial activities like funding research. That is one of the goals of DICARF.

Riedy and Hanus argue that data breaches would be well addressed through a compensation fund, but their proposal emphasizes the compensation fund as a substitute for litigation.[522] While a compensation fund reduces inefficiencies in litigation, it is not a replacement for litigation. Rather, compensation funds exist to improve the efficiency of compensating victims. Consider the

520. Riedy & Hanus, *supra* note 28, at 6–7.
521. *Id.* at 35.
522. *Id.* at 37.

lawsuit between a group of flight attendants and the tobacco industry that resulted in a settlement that set up a research fund to study secondhand smoke.[523] Participants in the lawsuit could still sue as individuals, but punitive damages would be unavailable. The defendants thus created a research fund in exchange for a limitation of liability.

Compensation funds might have the goal of addressing a massive disaster like the September 11th Victim Compensation Fund. A compensation fund also may be created when injuries cannot be traced to a specific bad actor, like the Vaccine Compensation Fund or Superfund sites identified for environmental cleanup under CERCLA. The Superfund model is also appealing because the fund is primarily used for cleanup costs to reduce future injuries. A trust fund similar to what exists for Superfund sites is one possible way of mitigating the high cost of data breach litigation.[524]

Ultimately, Riedy and Hanus make a compelling proposal for a data breach compensation fund, and this Article takes issue only with compensation funds being treated as a replacement for litigation rather than a complement. We also would prefer for the fund to serve a public interest purpose in addition to providing compensation for qualifying individual injuries. Using fines or settlements for data breaches to fund technology research would increase the overall efficiency of efforts to hold parties responsible for their actions and improve the overall security environment.

There is a lot of uncertainty when it comes to data breaches and their financial consequences. In this Article, we have argued that the injury and duty elements are easily established. That reduces some uncertainty, but the cost of litigation creates a significant encumbrance on parties that is disproportionate to the amount of damages awarded. Requiring businesses to pay their own attorney fees and possibly the attorney fees of plaintiffs as well adds inefficiencies in what should be a straightforward process. A compensation fund modeled after the Hazardous Substance Superfund Trust Fund could be used to improve conditions for everyone through the research of new technologies to reduce the global risk of data injuries.

VI. CONCLUSION

Data breaches and data misuse have wide-reaching effects, but the law has not quite caught up. In this Article, we focused on data breach lawsuits using a negligence framework. We argue for a legal duty to secure data and the recognition of data insecurity harms as injuries to autonomy. A legal duty to secure data is supported by statutory trends towards liability for people who were upstream or downstream of a data thief. We also posit that recognizing a duty to secure will significantly benefit the risk management process.

523. Rabin, *Enabling Torts*, *supra* note 182, at 450; *Broin*, *supra* note 504.

524. U.S. GOV'T ACCOUNTABILITY OFFICE, *Federal Fees, Fines, and Penalties* 10, (Dec. 1, 2016), https://www.gao.gov/assets/690/681352.pdf.

Data insecurity injuries are fundamentally injuries to autonomy and should be recognized as such. The erosion of privacy through neglect of security is troubling, and the legal system must shift away from traditional economic measurements of injury and focus instead on the fact that data insecurity is a social harm. The salt flats of Crait become a sea of red because we are no longer in control of our data prints. As a social harm, data injuries should be addressed collectively through class actions where appropriate, preferably in coordination with what would essentially amount to a crowdfunded computer security research fund. Our digital society can support a vibrant economic future, but legal uncertainty in security matters will certainly hobble progress.