THE SKELETON OF A DATA BREACH: THE ETHICAL AND LEGAL CONCERNS

Hilary G. Buttrick*
Jason Davidson**
Richard J. McGowan***

Cite as: Hilary G. Buttrick et al.,*The Skeleton of A Data Breach: The Ethical and Legal Concerns*, 23 Rich. J.L. & Tech. 2 (2016), http://jolt.richmond.edu/wp-content/uploads/volume23_article2_Buttrick.pdf.

INTRODUCTION

[1] After over thirty data breaches spanning the third and fourth quarter of 2012, Forbes magazine labeled the summer of 2012 as "The Summer of the Data Breach."[1] Four years later, businesses across multiple industries have suffered brand-image damage and paid millions of dollars in remedial expenses; we are living in the era of the mega breach.[2] In 2014, companies such as Target, Home Depot, JP Morgan Chase, Anthem, Sony, UPS, Jimmy John's, Kmart, Neiman Marcus, Community Health Systems, and the White House suffered data breaches.[3] The Home Depot

*J.D., Assistant Professor of Business Law, Butler University.

**M.B.A., Instructor of Management Information Systems, Butler University.

***Ph.D., Instructor of Business Ethics, Butler University.

[1] *See* Dave Lewis, *Notes from RSA: Accountability in Security*, FORBES, (Apr. 29, 2015, 6:30 PM), http://www.forbes.com/sites/davelewis/2015/04/29/notes-from-rsa-accountability-in-security/#47e46e292163, *archived at* https://perma.cc/HV4B-D7T8.

[2] *See* Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES, (Jan. 13, 2015, 7:06 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#4ad6aa5f3a48, *archived at* https://perma.cc/WYT4-8JX8.

[3] *See id.*; *see* Ellen Nakashima, *Hackers Breach Some White House Computers*, WASH. POST (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/hackers-

breach alone resulted in the loss of "56 million credit card accounts," "53 million email addresses," and an estimated 63 million dollars in damage.[4] In addition to the economic fallout associated with data breaches, the 2015 Ashley Madison data breach highlighted the personal toll faced by consumers when their "private" information becomes "public."[5] That data breach exposed the identities of millions of would-be philanderers, shaming not only the subscribers to Ashley Madison's service, but also innocent bystanders such as their family members.[6] The frequency of data breaches has shown no signs of abating in 2016—in the first quarter, multiple hospitals fell victim to "ransomware," a data breach that allows hackers to literally hold patient data hostage.[7] Several hospitals had to pay hackers to regain access to their patients' data.[8]

[2] "Decentralized technology" creates a different set of problems than the simple misuse of a single individual's "technological profile" and information.[9] Today, unauthorized access to electronic information, a result of what Burnham in 1983 referred to as "transactional information,"[10] includes "hackers breaking into systems or networks, third

breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html, *archived at* https://perma.cc/HD4S-MUX2.

[4] The Home Depot, Inc., Annual Report (Form 10-K) (Mar. 25, 2015), at 18–19.

[5] *See* Eric Basu, *Cybersecurity Lessons Learned from the Ashley Madison Hack*, FORBES, (Oct. 26, 2015, 11:55 AM), http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#14c58a7eed99, *archived at* https://perma.cc/U4L3-R6VE.

[6] *See id.*

[7] *See* Seung Lee, *Ransomware Wreaking Havoc in American and Canadian Hospitals*, NEWSWEEK, (Mar. 23, 2016, 10:23 AM), http://www.newsweek.com/ransomware-wreaking-havoc-american-and-canadian-hospitals-439714, *archived at* https://perma.cc/MJ2N-UW4T.

[8] *See id.*

[9] *See* Mary J. Culnan & Cynthia Clark Williams, *How Ethics Can Enhance Organizational Privacy: Lessons From the ChoicePoint and TJX Data Breaches*, 33 MIS Q. 673, 673 (2009).

[10] DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 50 (1983).

parties accessing personal information on lost laptops or other mobile devices, or organizations failing to dispose of personal information securely."[11] Data breaches exemplify the first type of unauthorized access and despite their frequent occurrence, they are little examined from an ethical standpoint. Though Google Scholar lists over 82,000 entries under "ethics of a data breach," very few combine both terms in the title.[12] One article that does so notes a "dearth of prior organizational-level privacy research, which has largely overlooked ethical issues or the personal harms often caused by privacy violations."[13] Even within the field of technology, "there has not been a huge literature on ethics within the mainstream of information systems journals."[14] Part of the problem is the novelty of data breach cases. They are so new and different that they appear to be technologically, morally, and legally unlike other problems. We suggest that analogies and analyses exist which can help resolve some of these moral and legal puzzles.

[3] First, this paper discusses the anatomy of a data breach, providing technical background on the way breaches occur. Next, we identify the ethical dimensions of data breaches. While privacy is a key topic in any ethical analysis of a data breach, other issues are more pressing, such as the responsibility of organizations to prevent and to repair consequences of data breaches. Then we analyze the current status of the law with regard to data breaches. We note immediately that the laws of various states are exactly that, various and eclectic. No consistent and stable legal understanding appears to have availed itself. The article concludes with guidance regarding data breach prevention, which can help businesses meet their ethical and legal obligations.

---

[11] Culnan & Williams, *supra* note 9, at 675.

[12] *See* Search Results for "Ethics of a Data Breach," GOOGLE SCHOLAR, https://scholar.google.com/scholar?hl=en&q=ethics+of+a+data+breach&btnG=&as_sdt=1%2C47&as_sdtp=, *archived at* https://perma.cc/7HZG-UK9D (last visited Sept. 20, 2016).

[13] Culnan & Williams, *supra* note 9, at 673.

[14] John Mingers & Geoff Walsham, *Toward Ethical Information Systems: The Contribution of Discourse Ethics*, 34 MIS Q. 833, 837 (2010).

I. DATA BREACH BASICS

[4] According to popular folklore, the first computer "bug" was officially documented in 1945.[15] This was years before the first personal computer was released, and instead of malware or social engineering deception, the "bug" was literally a moth that was stuck between two components of IBM's Harvard Mark II.[16] After a cataclysmic data breach in the modern computing age, however, postmortem reports eventually surface that provide the details of each individual breach.[17] These reports explain the hacker's methodology, the company's missed warning signs, and the collateral damage from the breach.[18] Each individual breach has its own signature as every data system is as unique as a fingerprint; however, these breaches generally occur in one of several ways.

[5] The most common and well-documented method of cyber-attack uses malware.[19] Malware, which includes viruses, worms, and trojan

[15] *See* Computerworld Staff, *The Moth in the Machine: Debugging the Origins of the Bug*, COMPUTERWORLD (Sept. 3, 2011, 7:00 AM), http://www.computerworld.com/article/2515435/app-development/moth-in-the-machine--debugging-the-origins-of--bug-.html, *archived at* https://perma.cc/KC3P-8QRF; *see also* Fred R. Shapiro, *Etymology of the Computer Bug: History and Folklore*, 62 AMERICAN SPEECH 376, 376–77 (1987).

[16] *See* Shapiro, *supra* note 15, at 376–77 (noting that a moth was found in the Mark II in 1945, but contending that the word "bug" was used to describe defects in machines long before 1945; thus, the term did not originate with the insect found in the Mark II).

[17] *See* Pragati Verma, *You've Been Breached -- What Now? A Post-Mortem Checklist*, FORBES: ALLCLEAR ID (Aug. 17, 2015, 11:27 AM), http://www.forbes.com/sites/allclearid/2015/08/17/youve-been-breached-what-now-a-post-mortem-checklist/#13a42ec34384, *archived at* https://perma.cc/Z365-VFCT.

[18] *See id.*

[19] *See* RAYMOND R. PANKO & JULIA L. PANKO, BUSINESS DATA NETWORKS AND SECURITY 91 (Pearson, 10th ed. 2015).

horses, is the "generic name for evil software." [20] A 2016 data breach report by Verizon found that malware continues to be the major contributor to data breaches involving stolen credentials and point of sale attacks. [21] Malware attacks, specifically worms, were publically credited for both the Target[22] and Home Depot[23] data breaches. Ironically, the first worm was created in 1975 by Xerox as a network analysis tool.[24] Modern day worms are standalone programs that can replicate and spread throughout a network when activated.[25] Some of the more notable worms include Melissa, ILOVEYOU, Slammer, and the Morris worm.[26] Malware is not the only factor that can lead to network compromise. Security breaches often are attributable to social engineering.[27]

---

[20] *Id.*

[21] *See* VERIZON, INC., 2016 DATA BREACH INVESTIGATIONS REPORT, at 20 (2016), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016, *archived at* https://perma.cc/E8S4-RHVU (follow "Download the 2016 DBIR") [hereinafter VERIZON REPORT].

[22] *See* Keith Jarvis & Jason Milletary, *Inside a Targeted Point-of-Sale Data Breach*, DELL SECUREWORKS, at 1 (Jan. 24, 2014), http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf, *archived at* https://perma.cc/5V6Y-CAED.

[23] *See* Hardekopf, *supra* note 2.

[24] *See* Michael A. Hiltzik, *Computer Viruses Can Be Healthy for Innovation*, L.A. TIMES (Apr. 5, 1999), at 1, http://articles.latimes.com/1999/apr/05/business/fi-24293, *archived at* https://perma.cc/A5ZD-P4R4.

[25] *See* PANKO & PANKO, *supra* note 19, at 93.

[26] *See, e.g.*, Ned Potter, *Top 10 Computer Viruses and Worms*, ABC NEWS (Sept. 3, 2009), http://abcnews.go.com/Technology/top-computer-viruses-worms-internet-history/story?id=8480794, *archived at* https://perma.cc/C6DW-YT2P (listing the top 10 most well-known computer viruses and worms).

[27] *See* VERIZON REPORT, *supra* note 21, at 17 (noting that most phishing cases "feature phishing as a means to install persistent malware," leading to security breach).

[6] Social engineering employs deception tactics to persuade the user to simply give the cybercriminal direct access to the system under attack, similar to the modus operandi of a traditional con-artist.[28] Social engineering attacks direct messages and correspondence to users who have access to the systems that are being attacked.[29] Through different methods of deception, the user is prompted to give away the information needed to access the system.[30] The most common methods of social engineering are spear phishing, smishing, and vishing.[31] Spear phishing is direct correspondence, usually via email, that is personally crafted to gain the trust of the end user.[32] Once trust is obtained, the user is prompted for login credentials and the system is compromised. Smishing and vishing are similar to spear phishing; however, they use text messages (smishing) and voice communication (vishing) as mediums.[33] It is also worth noting that old-fashioned tactics such as breaking and entering, removing files from the printer, or simply guessing passwords are still commonly used tricks of the trade.[34]

[28] *See* PANKO & PANKO, *supra* note 19, at 96–97.

[29] *See id.* at 96.

[30] *See id.* at 97.

[31] *See id.* at 96–97; *see* FBI, *Smishing and Vishing and Other Cyber Scams to Watch Out for This Holiday*, FEDERAL BUREAU OF INVESTIGATION (Nov. 24, 2010), https://archives.fbi.gov/archives/news/stories/2010/november/cyber_112410/cyber_112410 [hereinafter *Smishing and Vishing*].

[32] *See* PANKO & PANKO, *supra* note 19, at 97.

[33] *See Smishing and Vishing, supra* note 31.

[34] *See*, *e.g.*, Eric Geier, *Your Printer Could Be a Security Sore Spot*, PC WORLD (Apr. 25, 2012, 6:01 PM), http://www.pcworld.com/article/254518/your_printer_could_be_a_security_sore_spot.html, *archived at* https://perma.cc/7PZY-87MX (discussing five security threats network printers may impose); *see also* Matt Smith, *The 5 Most Common Tactics Used to Hack Passwords*, MAKE USE OF (Dec. 20, 2011), http://www.makeuseof.com/tag/5-common-tactics-hack-passwords/, *archived at* https://perma.cc/YJ4K-NDLR.

[7] To circumvent the millions of dollars companies invest in information technology security, hackers often use a combination of the tactics discussed above. As detailed in the Dell SecureWorks report on the Target infiltration, a combination of social engineering and malware was used to cause the collapse.[35] Hackers first targeted Fazio Mechanical Services, a vendor for Target.[36] They were able to gain login credentials through spear phishing, which in turn granted them direct access to the systems that opened a pathway to Target's network.[37] Upon accessing Target's data network, the hackers injected a worm into the system.[38] This worm compromised Target's point of sale systems using a customized version of malware called Black POS.[39] This malware then compromised Target's server, which allowed the data to be distributed and copied to servers located throughout the world; accordingly, the hack was very difficult to trace.[40]

[8] For businesses, the question of data breach is not "if" but "when." It is indisputable that the hackers in the examples discussed above bear the moral responsibility for their acts.[41] But the moral responsibility of the business that sustains the data breach presents a closer question. Businesses require consumers to provide their private information when completing even the most routine transactions; this places the business in a

[35] *See* Jarvis & Milletary, *supra* note 22, at 1,10.

[36] *See* STAFF OF S. COMM. ON COM., SCI., AND TRANSP., 113TH CONG., A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH 4 (2014), http://www.public.navy.mil/spawar/Press/Documents/Publications/03.26.15_USSenate.pdf, *archived at* https://perma.cc/SLX8-24UD.

[37] *See id.* at 8.

[38] *See id.* at 9.

[39] *See id.* at 2, 9.

[40] *See id.* at 4.

[41] *See generally* Richard J. McGowan & Hilary G. Buttrick, *Moral Responsibility and Legal Liability, or Ethics Drives the Law*, 11 J. LEARNING IN HIGHER EDUC. 9, 10 (2015) (discussing the three basic elements of moral responsibility).

unique position of trust. The scope of a business's moral responsibility for breach of that trust is discussed below.

II. MORAL RESPONSIBILITY AND DATA BREACH

[9] Of course, the right to privacy is at the fore. However, information technology "explicitly embodies particular important values…privacy, autonomy, universal usability, trust, and cooperation."[42] The existing literature does not explore the scope of a business' moral responsibility for data breach. Accordingly, reference to other areas, such as moral responsibility for marketing, is instructive. The values associated with information technology suggest moral analysis based on the ethics of marketing and on notions of corporate responsibility, inasmuch as knowledge plays a role in making autonomous choices and trust is associated with responsibility.[43]

[10] Three main positions have been staked out over the years with regard to marketing: the contractual view, the due care theory, and the social costs view, sometimes referred to as the "deep pockets" view.[44] Captured in the phrase, *caveat emptor,* the contractual view of the buyer-seller relationship holds that the seller, typically a business, only has the duties to the buyer that the contract states.[45] Thus, under the contract view, Ford could indeed sell a product which, when struck from behind at 21 miles per hour, could produce a flaming inferno.[46]

---

[42] Mingers & Walshman, *supra* note 14 at 839.

[43] *See generally* JOHN RAWLS, A THEORY OF JUSTICE 347–50 (1971) (discussing the moral psychology and the acquisition of the sentiment of justice).

[44] *See* MANUEL VELASQUEZ, BUSINESS ETHICS: CONCEPTS AND CASES 308 (7th ed. 2012).

[45] *See id.* at 314; *see generally* THOMAS GARRETT & RICHARD KLONOSKI, BUSINESS ETHICS 88 (2nd ed. 1986) (discussing the fairness of a sales contract and the importance of protecting the dignity of the buyers).

[46] *See generally* CLARK BUTLER, HUMAN RIGHTS ETHICS: A RATIONAL APPROACH 80 (2008) (discussing the moral psychology and the acquisition of the sentiment of justice).

[11] The problem is that consumers lack the knowledge that the producer has and therefore cannot act knowledgably in purchasing a product. The due care position recognizes the imbalance and the vulnerable position of the consumer by placing additional duties on the business.[47] As Culnan and Williams put the matter, "[w]e further argue that because consumers are vulnerable in their dealings with businesses due to information and control deficits, organizations have a moral duty—often overlooked, we observe—that extends beyond legal compliance requiring them to take reasonable precautions with consumer data and to avoid harm in using this data."[48] The "deep pockets" view–analogous to the legal notion of strict liability–would have the seller assume all costs–even when exercising "due care" to protect the consumer from risk and injury–of a product.[49] In other words, when a problem occurs, no investigation need be undertaken: the seller takes the responsibility, or *caveat vendor*.[50] Given the poor record of businesses with regard to handling data breaches,[51] the third option appears most reasonable.

[12] Corporations have been reluctant to take steps to exhibit moral responsibility in the area of data breach.[52] Normally, when wrongdoing occurs in an organizational setting, the elements of magnitude and

---

[47] S*ee* Edgar H. Schein, *The Problem of Moral Education for the Business Manager*, 8 INDUST. REV. 3, 4 (1966).

[48] Culnan & Williams, *supra* note 9, at 674.

[49] *See* Reed Dickerson, *The Basis of Strict Products Liability*, 16 FOOD, DRUG, COSMETIC L.J. 585, 591 (1961).

[50] *See* David A. Hall, *Strict Liability and Computer Software: Caveat Vendor*, 4 COMPUTER/L. J. 373, 373 (1983).

[51] *See generally* Culnan & Williams, *supra* note 9, at 681–82 (discussing the ways in which consumers are vulnerable when businesses lack appropriate data security measures); *see also* Simon Petravick & Stephan G. Kerr, *Protect Your Portable Data—Always and Everywhere*, 6 J. OF ACCT. 30, 31 (2009) (discussing the ways in which businesspeople often fail to appropriately safeguard confidential client information).

[52] *See* Culnan & Williams, *supra* note 9, at 681–82.

certitude of harm as well as connection and contribution to the harm are utilized.[53] Corporations appear to underestimate magnitude and certitude of harm and appear to ignore the contribution they make to data breaches by being primarily reactive rather than proactive.[54] While an analysis of a business's moral responsibility for a data breach suggests the appropriateness of a rule akin to strict liability, the law is far from imposing such an obligation.[55]

III. LEGAL LIABILITY AND DATA BREACH

[13] Not surprisingly, the development of data breach law has lagged behind the speed of technological innovation.[56] There are two significant legal questions surrounding data breaches. First, what legal obligations does a business owe its customers regarding data security and notifications of a breach? Second, what legal remedies do consumers have if their private information is compromised as the result of a data breach? As discussed below, there is currently no comprehensive federal regulatory scheme addressing data breach.[57] Instead, businesses must attempt to comply with a patchwork of state laws addressing data breach

[53] *See* McGowan & Buttrick, *supra* note 41, at 11.

[54] *See* Culnan & Williams, *supra* note 9, at 674.

[55] *See* Norman C. Simon, Brendan M. Schulman & Samantha V. Ettari, *Beware the Breach: Data Breaches, Notification Duties, and Legal Liability*, LEXOLOGY.COM (Aug. 29, 2012), http://www.lexology.com/library/detail.aspx?g=221e63eb-ccea-4f5f-80e7-b72905037a6f, *archived at* https://perma.cc/9FBG-KKQY.

[56] *See* Adi Snir, *Dealing with the Law Lag*, LEGALVISION (May 6, 2016), https://legalvision.com.au/dealing-with-the-law-lag/, *archived at* https://perma.cc/7SW7-4KFE.

[57] *See* Peter J. Arant, *Understanding Data Breach Liability: The Basics Every Attorney Should Know*, 40 MONT. L. 8, 8–9 (2015) ("At the federal level, there is no comprehensive data privacy or security law. Instead the U.S. follows a 'sectoral' approach, meaning there are federal laws that apply to specific sectors.").

notifications.[58] Additionally, consumers are left with few effective civil remedies when their private information is breached.[59]

A. Data Breach Notification Laws

[14] At present, there is no comprehensive federal statute addressing a business's obligation to safeguard personal information.[60] While there are a few federal statutes aimed at protecting personal information in narrow contexts (such as the protection of medical and health-related information under the Health Insurance Portability and Accountability Act of 1996),[61] the legal rules governing data breach are handled largely at the state level.[62] Currently, "[f]orty-seven states, [and] the District of Columbia"

[58] *See id.*; *see also Comparison of U.S. State and Federal Security Breach Notification* Laws, STEPTOE & JOHNSON LLP (Jan. 21, 2016), http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf, *archived at* https://perma.cc/4R39-6XJQ.

[59] *See* Rachel M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1175 (2014) ("[O]nce an individual has been notified of a breach, she has limited legal recourse against the company or organization that exposed her personal information.").

[60] *See* Arant, *supra* note 57, at 8–9.

[61] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; *see* Arant, *supra* note 57, at 9 (noting that the Federal Trade Commission may bring lawsuits against companies with "lax security and privacy practices" because they are considered "unfair or deceptive practices"); *see also* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 47, 53–54 (2015) ("Because no federal law in the United States provides a broad, comprehensive set of data breach notification or data protection requirements for all businesses and consumers, other federal administrative bodies have provided catch-all protection in some circumstances.").

[62] *See* Jeff Kosseff, *Cyberwars: Navigating Responsibilities for the Public and Private Sector: Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 402 (2016) (We have "a patchwork of related laws, including breach notification and privacy statutes, that focus on penalizing companies for inadequate data security. But our legal system lacks a coordinated network of laws that are designed to promote cybersecurity and prevent data breaches from occurring in the first place."); *see also* Peters, *supra* note 59, at 1181 (discussing various state law data-breach notification statutes).

have laws addressing business obligations with regard to data breaches.[63] Three states—Alabama, New Mexico, and South Dakota—have no statutes on the books addressing consumer notification of data breaches.[64] Most states impose obligations on businesses to maintain "reasonable security" measures "to protect personal information."[65] While definitions vary from state to state, "personal information" commonly includes an individual's social security number,[66] or

> [A]n individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.[67]

[15] A "breach" occurs when there is an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. . . ."[68]

---

[63] *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, *archived at* https://perma.cc/8JUS-CXX5 [hereinafter NCSL Security Breach Research]

[64] *See id.*

[65] Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, 21 J.L. & TECH. 1, 14 (2015) (explaining general state law requirements for data breach security in context of attorneys' obligations to secure data).

[66] *See* IND. CODE § 24-4.9-2-10(1) (2014).

[67] IND. CODE § 24-4.9-2-10(2)(A)-(D) (2014).

[68] IND. CODE § 24-4.9-2-2(a) (2014).

[16] In the event of a data breach, existing statutes require businesses to provide some type of notification to the consumer.[69] The type and timing of that notice, however, varies from state to state.[70] Some states require consumer notification whenever unauthorized access of personal information occurs.[71] Other states require businesses to notify consumers only if there appears to be a reasonable risk that some harm will result from the breach.[72] Many states require businesses to notify the attorney general of data breaches.[73] Some statutes require notification within a specified time frame, while others simply require that notification be done expediently.[74] Businesses that serve consumers in multiple states must comply with the notification requirements of each of the states where affected consumers reside.[75] Thus, when a large data breach occurs, businesses face a considerable challenge in ensuring compliance with the various notification laws throughout the country.[76]

[17] This patchwork of state regulation leads commentators and policy advocates to suggest that a comprehensive federal data breach statute

[69] *See* NCSL Security Breach Research, *supra* note 63.

[70] *See Data Breach Charts,* BAKER HOSTETLER 1, 17–18, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf, *archived at* https://perma.cc/MM5K-ZRT3 (last visited Oct. 4, 2016) (providing state-by-state-survey of data breach notification requirements).

[71] *See id.* at 9.

[72] *See id.* at 9–12.

[73] *See id.* at 13–16.

[74] *See id.* at 15-16, 18–19.

[75] *See* Sasha Romanosky et al., *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 80 (2014) ("[I]t is the residence of the individual that drives disclosure, not the location of the breach. That is, disclosure to an individual is required only if the state in which the individual is a citizen has adopted a disclosure law.").

[76] *See* Arant, *supra* note 56, at 10 ("Given the heterogeneous nature of state data breach notification laws, simultaneous compliance with multiple laws can be a logistical nightmare—and an expensive one at that.").

should be enacted.[77] A federal data breach statute would preempt state regulation, thus simplifying the breaching business's compliance requirements and costs.[78] Instead of struggling to comply with the various notification laws of multiple states, a business would look to only one source—federal law—to discern its obligations in the event of a data breach.[79] While federal bills have been proposed,[80] Congress has failed to pass any comprehensive proposal.[81]

[18] Moreover, critics claim that draft bills are weak and do not offer enough protection for consumers.[82] In particular, critics note that the

[77] *See* Jill Joerling, Note, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467, 486 (2010) ("Congress should take action immediately to enact a federal data breach notification law."); *see also* Jay P. Kesan, *et al*., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 346–48 (2016) (suggesting "a complete overhaul of data privacy law[s] and the creation of [centralized] profile repository" for consumers' data that would operate in a fashion similar to credit bureaus); Tschider, *supra* note 61, at 72 ("a federal statute should regulate all businesses involving consumer personal information to effectively preserve customer choice and control with respect to their information, to drive contract efficiency, and to facilitate international trade.").

[78] *See* Joerling, *supra* note 77, at 486.

[79] *See id.* ("Replacing the current patchwork of . . . state laws with a single comprehensive federal law would give businesses a clear road map to follow after a breach.").

[80] *See*, *e.g.*, Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. (2d Sess. 2016) (demonstrating a proposed federal data breach law that did not pass in Congress).

[81] *See* Brett V. Newman, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 U. Ill. J.L. Tech. & Pol'y 437, 445 (2015) ("The patchwork state legislation and numerous bill introduced in Congress show how difficult it is to agree on breach notification and data security measures. There is likely an agreement that the United States needs a data breach law, but that does not mean that one will be passed. The problem may also come from a surplus of Congressional committees claiming jurisdiction and trying to tackle the issue—resulting in too many different bills.").

[82] *See* Peters, *supra* note 59, at 1196. (Although Peters analyzes an earlier draft bill, the Data Security & Breach Notification Act of 2013, her criticism holds true for the Data Security Breach Notification Act of 2015.)

proposals do not do enough to incentivize data breach prevention because they focus on consumer notification after a breach has already occurred.[83] To incentivize data breach prevention, businesses must view added security measures as solid investments that minimize risks of loss.[84] The primary business risks associated with data breaches are loss of customer goodwill and, of course, lawsuits from affected consumers.[85] As discussed below, data breach lawsuits are difficult to pursue. Accordingly, the threat of consumer litigation has not played an extensive role in influencing businesses to adopt more stringent security measures.[86]

B. Consumer Remedies for Data Breach

[19] Some commentators have argued that in order to meaningfully encourage businesses to adopt better data protection measures, businesses must view customer litigation as a serious threat.[87] The threat of litigation in this context has been largely hollow because consumers have few legal

[83] *See id.*; *see also* Tschider, *supra* note 61, at 74–75 (emphasizing the need for a federal law that focuses on data protection in addition to data breach notification: "Having clear data protection standards will dramatically reduce uncertainty for consumers and business, as standard data protection requirements will be articulated and required for implementation . . ."); s*ee also* Andrea Peterson, *Why this National Data Breach Notification Bill has Privacy Advocates Worried*, WASH. POST (Apr. 15, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/04/15/why-this-national-data-breach-notification-bill-has-privacy-advocates-worried, *archived at* https://perma.cc/C9U3-S3W3 (noting that consumers could have fewer protections under Data Security Breach Notification Act of 2015 than they have under existing state laws).

[84] *See* Kosseff, *supra* note 62, at 403 (arguing that laws should create incentives through tax credits and litigation safe harbors to encourage businesses to invest in cybersecurity infrastructure; rather than focus solely on penalties for data breaches).

[85] *See* PONEMON INST., 2016 COST OF DATA BREACH STUDY: UNITED STATES, IBM, 1, 3, 13 (2016).

[86] *See* Peters, *supra* note 59, at 1193.

[87] *See id.* at 1197 (noting that a national data breach law that gives consumers a private right of action or requires mandatory credit monitoring "will be an incentive for companies to minimize data breaches.").

remedies when their personal information is breached.[88] While data breach statutes require businesses to notify consumers in the event of a breach, only a handful of those statutes create a private cause of action that allows the consumer to bring a lawsuit against the business.[89] Thus, in the majority of states with data breach statutes, the consumer is statutorily entitled to notice of the breach but little else.[90] Given the lack of meaningful statutory remedies for data breaches, consumers have looked to the common law for a cognizable theory of recovery.[91] Consumers have sought damages for data breaches under theories of negligence, breach of contract, breach of fiduciary duty, and infliction of emotional distress.[92] These common law theories are not well-suited to data breach cases and often end in dismissal for several reasons.[93]

[20] First, the harm that results from data breaches is most commonly economic harm—there is no personal injury or physical property damage sustained by the consumer as a result of the data breach.[94] Many

[88] *See, e.g.*, Nicole Hong, *For Consumers, Injury Is Hard to Prove in Data-Breach Case*, WALL ST. J. (June 26, 2016, 8:06 PM), http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988, *archived at* https://perma.cc/F3VF-8LKD.

[89] *See* BAKER HOSTETLER, *supra* note 70, at 16–18.

[90] *See* Kesan *et al*., *supra* note 77, at 277 (noting that "many other states merely require companies to notify customers of data breaches and the relevant statutes do not create any additional duties or entitlements.").

[91] *See also* Thomas Martecchini, *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, 1474 (noting that courts are divided on "whether increased risk of identity theft is an injury-in-fact sufficient to create standing…").

[92] *See* Peters, *supra* note 59, at 1185 (discussing various common law theories available to consumers for data breach).

[93] *See id.* at 1185–87 ("[A] principle reason that civil causes of action in data-breach cases are rarely successful is the difficulty consumer data-breach victims have in meeting the standing and injury requirements.").

[94] *But see* Kesan *et al*., *supra* note 77, at 344 (discussing the various types of harm that result from loss of control over personal data, "including dignitary harms; a chilling

jurisdictions follow a rule called the "economic loss doctrine," which prevents consumers from recovering purely economic damages under a tort theory (such as negligence or infliction of emotional distress).[95] Thus, in jurisdictions that follow the economic loss doctrine, data breach claims sounding in tort rarely reach the jury because they are dismissed as the result of pretrial dispositive motions filed by the defendant.[96]

[21] Second, many data breach cases are dismissed because the consumer lacks standing to bring such a claim.[97] Standing is a constitutional prerequisite to litigation that requires the plaintiff to have suffered an injury in fact.[98] In other words, the harm sustained by the plaintiff must be real, not hypothetical or speculative.[99] In data breach cases, the injury can be hard to define. Plaintiff consumers often argue that the data breach itself and the risk of future identity theft are sufficient harms; defendant businesses contend that no injury has occurred unless the plaintiff can show a link between the data breach and an actual instance of

effect from law enforcement having too much control over individual expression; and circumstances that interfere with an individual's ability to exercise freedoms or develop a sense of self-determination.").

[95] *See, e.g.*, Gunkel v. Renovations, Inc., 822 N.E.2d 150, 154 (Ind. 2005) (holding that economic losses are not recoverable in a tort action premised on the failure of a product or service to perform as expected unless the failure results in personal injury or physical harm to property other than the product; proper remedy sounds in contract).

[96] *See* Peters, *supra* note 59, at 1186 (discussing data breach cases dismissed on economic loss grounds).

[97] *See id.* at 1187 (discussing split of authority with regard to whether consumers have standing to bring suit in data breach cases).

[98] *See, e.g.*, Remijas v. Nieman Marcus Group, LLC, 794 F.3d 688, 691–92 (7th Cir. 2015) (holding that standing requires a litigant to show a concrete injury that is causally linked to the defendants conduct and can be redressed by the court).

[99] *See id.*

identity theft.[100] Not surprisingly, the courts are divided on what type of injury suffices to confer standing in a data breach case.[101]

[22] Even if the plaintiff consumer in a data breach case survives the standing hurdle, he or she must still prove all of the elements of his or her case in order to win. In most instances, the consumer will have to prove that his or her injury was caused by the defendant's data breach.[102] Proving causation in data breach cases can be difficult because the plaintiff's personal information may have been compromised in other data breaches, making it nearly impossible to establish that the suffered identity theft was solely the result of the defendant's breach.[103]

[23] The procedural and substantive difficulties associated with data breach litigation mean that very few of these cases are likely to survive dispositive motions and reach a jury, which in turn makes them less attractive to class action attorneys.[104] The procedural hurdles, the cost of litigation, and the prospect of a small recovery are enough to deter most individual consumers from bringing a data breach lawsuit.[105] Without

[100] *See* Peters, *supra* note 59, at 1189–92 (collecting cases addressing standing and injury-in-fact in context of data breach litigation).

[101] *See id.*; *see also* Martecchini, *supra* note 91, at 1474 (noting that courts are divided on "whether increased risk of identity theft is an injury-in-fact sufficient to create standing…").

[102] *See* 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, 685–86 (2016) (discussing difficulties of applying common law tort theories to data breach cases).

[103] *See* Peters, *supra* note 59, at 1188 ("[I]f a person is the victim of two or more data breaches in which similar personal information is stolen and that information is not used until years later to harm her, it may be difficult for the victim to demonstrate which breach was the source of the information used."); *see also* Newman, *supra* note 81, at 440 ("proving that a customer lost money due to a specific breach can be difficult.").

[104] *See* Peters, *supra* note 59, at 1192–93.

[105] *See generally* Jeff John Roberts, *This Court Ruling Just Made It Easier to Sue Companies That Get Hacked*, FORTUNE (July 29, 2015, 7:00 PM), http://fortune.com/2015/07/29/data-breach-7th-circuit/, *archived at*

effective legal remedies, most consumers must simply put up with the headaches associated with data breaches.[106] While external litigation pressures and the current data breach regulatory state may not incentivize businesses to take additional steps to safeguard consumer privacy, ethics would certainly suggest that businesses should voluntarily adopt higher standards for data protection.[107]

IV. BUSINESS STRATEGIES TO MINIMIZE THE RISK OF DATA BREACH

[24] Several tactics can help reduce the threat of cybercrime. The first tactic is infrastructure.[108] A modern company must continually perform routine maintenance including, but not limited to, security patches, operating system upgrades, and hardware upgrades. Often cyber criminals exploit older software to maliciously gain access to data networks.[109] The initial discovery of these exploits before the software manufacturer has developed a security patch is called a "zero-day attack."[110] Once a hardware or software exploit is identified, software and hardware vendors act to create patches to repair the problem as quickly as possible.[111] It is up to the corporation to obtain and apply these patches.

---

https://perma.cc/C4ZT-SQD7 (discussing the hurdles victims of data breaches face when trying to sue).

[106] *See* Simpson, *supra* note 102, at 698 (observing that "the average consumer is essentially at the mercy of a breached entity's largesse to gain any recompense for stolen data.").

[107] *See supra* Part II; *see also* Martecchini, *supra* note 91, at 1473 (noting that while many businesses are implementing data protection plans, "many other businesses still remain in denial about the threat of data breaches, either failing to implement any data-security changes or making only nominal modifications.").

[108] *See* Pierluigi Paganini, *Preventing and Recovering From Cybercrime*, TRIPWIRE (Nov. 4, 2014), http://www.tripwire.com/state-of-security/incident-detection/preventing-and-recovering-from-cybercrime/, *archived at* https://perma.cc/PYB7-VKN5.

[109] *See* PANKO & PANKO, *supra* note 19, at 92.

[110] *See id.*

[111] *See id.*

[25] The second prevention method is active monitoring.[112] Similar to the way that the FBI manages the national threat level, a company's IT department must manage the cybercrime threat level.[113] Myriad firewall and IT monitoring software is available to monitor network traffic.[114] Many anti-virus software programs automatically scan and remove commonly found malware.[115] In addition, IT security companies provide external monitoring services to augment a company's internal monitoring procedures.[116] These offsite IT services offer network traffic monitoring and even provide built-in client insurance/reimbursement if a data breach occurs due to negligence within their services.

[26] The third prevention method is education.[117] While most people envision a hacker in a dark basement surrounded by computers, social engineering is a remarkably effective method of data intrusion.[118] For example, a study of data breaches occurring in 2015 found that "30% of phishing messages were opened by the target across all campaigns."[119] The risk of data breach can be mitigated if employees know they should never share passwords; they should frequently change passwords, and they

[112] *See* Paganini, *supra* note 108.

[113] *See DC Metro Cyber Security Summit*, THE CYBERWIRE (June 3, 2015), https://www.thecyberwire.com/events/dc-metro-cyber-security-summit-2015.html, *archived at* https://perma.cc/Z4XN-M6NK.

[114] *See, e.g.*, PANKO & PANKO, *supra* note 19, at 116–23 (discussing various forms of firewalls, their strengths, and their weaknesses).

[115] *See id.* at 124.

[116] *See, e.g.*, *Third Party Monitoring - Vendor Monitoring*, OBSERVEIT, http://www.observeit.com/solutions/third-party-monitoring, *archived at* https://perma.cc/P3SX-SW4W (last visited Sept. 23, 2016) (illustrating the monitoring services that a third party security company provides).

[117] *See* Paganini, *supra* note 108.

[118] *See* VERIZON REPORT, *supra* note 21, at 17.

[119] *Id.* at 18.

should lock their office doors.[120] Additional security measures such as key fobs, biometric readers, and similar devices that must remain with employees, should also be kept private. While no one strategy can guarantee that a business will not sustain a data breach, the preceding measures will lessen the risk.

V. CONCLUSION

[27] Though data breaches are a relatively new phenomena, guidance about the technology, morality, and legality of data breaches is available. If we are correct, corporations must do a better job of determining where data breaches are likely to occur, whether from human error or informational system flaw. Corporations must take steps to minimize risk before data breaches occur. Protocols must be put in place that assume responsibility for the consumers' negative consequences, such as notifying them immediately and providing help in diminishing the harm from the data breach. The legal liability will be mitigated; trust and cooperation will more likely flourish.

[120] *See generally* JERRY FITZGERALD, ALAN DENNIS & ALEXANDRA DURCIKOVA, BUSINESS DATA COMMUNICATIONS AND NETWORKING 362 (11th ed. 2012) (noting that security policies should explain to employees how to control the risk of intrusion).