THE PATCHWORK PRIVACY PROBLEM: HOW THE UNITED STATES' PRIVACY REGIME FAILS TO PROTECT ITS BUSINESSES AND DATA SUBJECTS

*Christopher Cozzens**

I. INTRODUCTION

As a civilization, the modern world is generating a plethora of data, and the rate of generation is compounding rapidly. As of 2013, 4.4 zettabytes of data made up the digital universe, and it was projected that this number could expand to 44 zettabytes of data by the end of 2020.[1] For perspective, streaming 44 zettabytes of high-definition-quality (HD) video would take approximately 572 million years.[2] The growth rate can be described as exponential, with 90 percent of the world's data generated in the last two years alone.[3]

The world generating more data is a direct result of each individual generating data at increasing speeds. Each person generates a substantial amount of data each day; every person generated an estimated 1.7 megabytes (MB) of data each second during 2020.[4] For scale, the original Super Mario Bros. video game, released in 1985,[5]

* J.D. Candidate, Seton Hall University School of Law, 2022; B.A., University at Buffalo 2013. I would like to thank Professor David Opderbeck for his thoughtful guidance throughout my Comment-writing process. I would also like to thank the members of the *Seton Hall Law Review* for their friendship, comradery, and support over the last two years.

[1] EMC DIGIT. UNIVERSE, THE DIGITAL UNIVERSE OF OPPORTUNITIES: RICH DATA AND THE INCREASING VALUE OF THE INTERNET OF THINGS (2014), https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

[2] Bernard Marr, *Big Data: What is a Brontobyte?*, WORLD ECON. F. (Feb. 12, 2015), https://www.weforum.org/agenda/2015/02/big-data-what-is-a-brontobyte/ (calculating 1 petabyte of HD video would last 13 years).

[3] Jacquelyn Bulao, *How Much Data is Created Every Day in 2020?*, TECH JURY: BLOG, https://techjury.net/blog/how-much-data-is-created-every-day/ (last updated Feb. 6, 2022).

[4] *Id.*

[5] Chris Plante, *When was Super Mario Bros. Released in the US? Nobody Knows!*, VERGE (Sept. 14, 2015, 2:20 PM), https://www.theverge.com/2015/9/14/9324833/super-mario-brothers-30th-anniversary-date.

which contained 32 independent and in-depth levels,[6] had a total original file size of 32 kilobytes.[7] That equates to .032MB, 53 times smaller than the amount of data a person generated each *second* in 2020.

As we generate more data, technology is evolving to process that data at accelerating rates. According to Moore's Law, the computer processing speed was projected to double every two years, but that estimate has proven conservative, with the processing instead doubling every 18 months.[8] Moore's Law "is just one manifestation of the greater trend that all technological change occurs at an exponential rate."[9] Some commentators have posited that in the 21st century, we could experience "20,000 years of progress (at today's rate)."[10] As the technology field expands at a shocking pace, statistically speaking, consumers, businesses, and other data generators are exposed to more cybercrime than ever before.

Data breaches pose one of the biggest cybersecurity threats. Data breaches have become more prevalent in recent years, exposing consumers to an increased risk that their personal information will be exposed to nefarious hackers.[11] According to the Privacy Rights Clearinghouse, an organization dedicated to protecting privacy, there have been over 9,000 reported data breaches since 2005.[12] The real number is likely magnitudes higher as this data does not include unreported breaches or breaches that do not involve U.S. citizens.[13] In

---

[6] *Super Mario Bros.*, NINTENDO WIKI, https://nintendo.fandom.com/wiki/Super_Mario_Bros (last visited Oct. 11, 2020).

[7] Preston Phro, *More Mario Trivia Than You Can Fit in King Koopa's Castle*, SORANEWS24 (July 9, 2014), https://soranews24.com/2014/07/09/more-mario-trivia-than-you-can-fit-in-king-koopas-castle [https://web.archive.org/web/20210113134429/https://soranews24.com/2014/07/09/more-mario-trivia-than-you-can-fit-in-king-koopas-castle/].

[8] *Moore's Law*, ENCYC. BRITANNICA, https://www.britannica.com/technology/Moores-law (last updated Dec. 26, 2019).

[9] *Big Idea: Technology Grows Exponentially*, BIG THINK (Mar. 21, 2011), https://bigthink.com/think-tank/big-idea-technology-grows-exponentially.

[10] *Id.*

[11] *See, e.g.*, Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN: DATA INSIDER BLOG (Dec. 1, 2020), https://digitalguardian.com/blog/history-data-breaches ("In 2005 alone, 136 data breaches were reported by the Privacy Rights Clearinghouse. . . . [However,] the 2015 Verizon Data Breach Investigations Report covered over 2,100 data breaches in which more than 700 million records were exposed for the year 2014 alone.").

[12] *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://privacyrights.org/data-breaches (last visited Nov. 10, 2020) (downloaded data set and summed the total rows, each row represents one data breach).

[13] Abi Tyas Tunggal, *116 Must-Know Data Breach Statistics for 2021*, UPGUARD: BLOG, https://www.upguard.com/blog/data-breach-statistics (last updated Dec. 5, 2021).

2019 alone, there were 1,473 reported data breaches.[14] In total, those breaches consisted of over 10,387,398,893 customer records.[15] Even more shocking, a cyberattack occurs every thirty-nine seconds,[16] and some commentators predict that a business will fall victim to a ransomware attack every two seconds by 2031.[17] At this alarming rate, it is not a matter of if your data will be stolen, but when.

Once data is breached, the costs start stacking up for the affected business. It is estimated that the average cost of a data breach in the United States is $7.91 million to the affected business.[18] "Studies show 29% of businesses that face a data breach end up losing revenue.[19] Of those businesses, 38% experience a loss of 20% of [sic] more."[20] This lost revenue is likely a side effect of the reputational harm associated with a data breach.[21] Depending on the severity, data breaches can result in a complete loss of data, which can force companies to shut down operations.[22] The longer operations stop, the more likely the business will suffer greater reputational harm and revenue impact.[23]

---

[14] J. Clement, *Cyber Crime: Number of Breaches and Records Exposed 2005-2020*, STATISTA (Oct. 1, 2020), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://web.archive.org/web/20201206081157/https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/].

[15] *Data Breaches*, *supra* note 12. In total, the Privacy Rights Clearinghouse database shows those breaches comprised of 10,387,398,893 customer records. *Id.*

[16] Michel Cukier, *Study: Hackers Attack Every 39 Seconds*, UNIV. OF MD. A. JAMES CLARK SCH. OF ENG'G: NEWS (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. For a discussion on the differences between cyber attacks and data breaches, see Tom Webley & Philip Thomas, *Crisis Management: Data Breaches and Cyber Attacks*, REED SMITH: PERSPECTIVES BLOG (Dec. 17, 2019), https://www.reedsmith.com/en/perspectives/2019/12/crisis-management-data-breaches-and-cyber-attacks ("A cyber attack is broader than a data breach, is deliberate and can be more disrupting to business.").

[17] Sam Cook, *2018-2022 Ransomware Statistics and Facts*, COMPARITECH (Jan. 28, 2022) https://www.comparitech.com/antivirus/ransomware-statistics/.

[18] Ryan Brooks, *What to Know About a Data Security Breach*, NETWRIX: BLOG, https://blog.netwrix.com/2018/11/29/what-to-know-about-a-data-breach-definition-types-risk-factors-and-prevention-measures/ (last updated Jan. 13, 2022).

[19] Maddie Davis, *4 Damaging After-Effects of a Data Breach*, CYBINT (July 25, 2019), https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach/.

[20] *Id.*

[21] Doug Drinkwater, *Does a Data Breach Really Affect your Firm's Reputation?*, CSO (Jan. 7, 2016, 3:55 AM), https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html (referencing a survey "conducted by OnePoll, [finding] 86.55 percent of 2,000 respondents stated that they were 'not at all likely' or 'not very likely' to do business with an organization that had suffered a data breach involving credit or debit card details").

[22] Davis, *supra* note 19.

[23] *See id.*

Additionally, survey research shows that in the event of a breach, consumers are quick to turn their backs, with 65 percent of data breach victims reporting lost trust in an organization as a result of a breach.[24] "Additionally, 85% [of consumers] will likely tell others about their negative experience, with 33.4% using social media and 20% commenting directly on a company website."[25] All of this leads to a troubling result: 60 percent of small businesses impacted by a data breach close their doors within six months of an attack.[26] Furthermore, because small businesses tend to be easier to attack, they are the victims of 60 percent of hacks.[27] From the business side of a data breach, the goal of data breach legislation should focus on minimizing data breaches to protect smaller businesses.

While the damages to businesses are concerning, the damages to the affected data subjects are shocking. By 2018, two-thirds of people online have had their records stolen or compromised by bad actors.[28] Many data subjects have already had their data accessed multiple times. For example, utilizing a recent calculator produced by the New York Times,[29] between 2005 and 2019, *my* personal:

- home address was accessed six times;
- credit card information was accessed four times;
- date of birth was accessed five times;
- email was accessed nine times;
- employment history was accessed once;
- financial history was accessed once;
- name was accessed ten times;
- passport number was accessed once;
- passwords were accessed eight times;

---

[24] CENTRIFY, THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE 12 (2017), https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf.

[25] Davis, *supra* note 19; *see also Interactions Finds 45 Percent of Shoppers Don't Trust Retailers to Keep Information Safe*, INTERACTIONS (June 26, 2014), https://www.interactionsmarketing.com/press-releases/interactions-finds-45-percent-of-shoppers-dont-trust-retailers-to-keep-information-safe/ [https://web.archive.org/web/20210201005417/https://www.interactionsmarketing.com/press-releases/interactions-finds-45-percent-of-shoppers-don't-trust-retailers-to-keep-information-safe/].

[26] *Id.*

[27] *Data Security Breach: 5 Consequences for Your Business*, AME GRP., https://www.theamegroup.com/security-breach/ (last visited Feb. 8, 2021).

[28] CTR. FOR STRATEGIC & INT'L STUD., ECONOMIC IMPACT OF CYBERCRIME: NO SLOWING DOWN 4 (2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

[29] K.K. Rebecca Lai et al., *How Many Times Has Your Personal Information Been Exposed to Hackers?*, N.Y. TIMES (July 30, 2019), https://www.nytimes.com/interactive/2015/07/29/technology/personaltech/what-parts-of-your-information-have-been-exposed-to-hackers-quiz.html.

- cellphone number was accessed seven times; and
- social security number was accessed twice.[30]

The rate that consumers experience data breaches is intensifying rapidly year after year. The total number of identity theft and fraud complaints increased from 2.9 million in 2017 to 4.7 million in 2020.[31] Thus, the chances are high that your personal information is already in the hands of immoral actors.

Furthermore, data breaches often lead to much more harmful consequences. Experian has published statistics showing that 31 percent of data breach victims later have their identity stolen.[32] "There is a new victim of identity theft every two seconds in the United States alone."[33] These consumers reported $905 million in total fraud losses in 2017, a 21.6 percent increase from 2016.[34] This equates to a median loss of $429.[35] Once the data subject learns that they have been exposed to a breach, they must decide how to protect themselves, which some commentators believe is impossible.[36] Data subjects will face a series of challenges, in part, because of the current patchwork privacy regime in the United States.

This Comment will examine the current landscape of data breach legislation to identify how data breach legislation contributes to the startling statistics outlined above, and how data breach legislation poses problems for data subjects and businesses alike. Specifically, this Comment will propose a federal privacy law that identifies reasonable security measures that businesses can comply with to prevent data breaches. Such a law should provide a private right of action if those measures are not met. Part II will provide a general overview of the current patchwork privacy regime in the United States and discuss the current framework of data breach privacy legislation. Next, Part III will discuss the difficulties businesses inevitably run into when attempting to comply with fifty different state statutes. Part IV will look to the private right of action provisions, or lack thereof, in several state

---

30 *Id.*

31 *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 18, 2022).

32 Matt Tatham, *Identity Theft Statistics*, EXPERIAN (Mar. 15, 2018), https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

33 *All Data Breaches in 2019 & 2020 – An Alarming Timeline*, SELFKEY (Jan. 8, 2019), https://selfkey.org/data-breaches-in-2019/.

34 Tatham, *supra* note 32

35 *Id.*

36 *See* Lai et al*., supra* note *29* ("How can you protect yourself in the future? It's pretty simple: You can't.").

statutes to identify multiple discrepancies and gaps in protections that often leave data subjects bearing the costs of privacy. Finally, Part V will propose a federal solution to address the ambiguity by advocating for a federal private right of action. Furthermore, Part V will look to existing "sectors" to identify measures that businesses should take to prevent data breaches and better protect both themselves and data subjects. In sum, this Comment will first advocate for a solution that shifts the costs of privacy from the data subject to businesses and, provides businesses with reasonable guidelines to increase data security, thereby decreasing data breaches and the overall "cost" of privacy in the future.

II. THE UNITED STATES' SECTORAL APPROACH TO FEDERAL PRIVACY LAWS AND THE PATCHWORK OF STATE LAWS FOR DATA BREACH NOTIFICATIONS

A brief analysis of the current United States privacy system uncovers several key issues that should be addressed. This Part will outline the high-level framework of the privacy rights afforded to United States citizens.

Starting broadly, there is no right to privacy in data conveyed to third parties.[37] The American legal system has typically denied legal rights for data privacy and instead relies on self-regulation and the litigation process to dictate appropriate behavior in society.[38] Any protections that exist for information privacy are generally assembled from a combination of narrowly targeted rules.[39] The combination of these specific rights leaves substantial gaps resulting in fewer clear remedies for violations of reasonable information practices.[40]

But the prevailing mindset may be shifting. In *United States v. Jones*, Justice Sotomayor stated in a concurring opinion that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[41] Justice Sotomayor specifically noted that this reconsideration might be necessary because of the context of the digital age, where people provide a plethora of information about themselves to third parties every day.[42]

The increased focus on privacy should also expand in the context of data collected by businesses. In the business environment, because

---

[37] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[38] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877 (2002).

[39] *Id.*

[40] *Id.*

[41] *Jones*, 565 U.S. at 417.

[42] *Id.*

of the accelerating speed at which data is collected and the amount of data collected during this process, the data collected by third parties is more closely analogous to data stored on a cell phone[43] rather than the trash in your trash bin[44] or bank-statements.[45] Because the amount of data collected is enormous, it is time to reconsider the notion that an individual does not have a right to data privacy.

While there is no general constitutional right to data privacy, legislative rights exist. Generally, privacy in the United States is governed by a patchwork of state and federal laws.[46] Federal privacy statutes in the United States follow a sectoral approach to privacy which is governed by various regulations covering specific industries such as the Gramm-Leach-Bliley Act (GLBA) for financial institutions,[47] Health Insurance Portability and Accountability Act (HIPAA) for the medical industry,[48] and Family Educational Rights and Privacy Act (FERPA) for the education field.[49] While at first there were many gaps between sectors that left some companies unregulated entirely, today, larger companies may be regulated by multiple sectors, creating confusion and causing complicated compliance requirements.[50]

In addition to the federal regulation of certain sectors, states have enacted privacy statutes with various degrees of protection, including individual data breach notification statutes. Data breach state legislation has been rapidly evolving throughout the United States. The

---

[43] *See generally* Riley v. California, 573 U.S. 373 (2014) (holding that a search of a cell phone incident to arrest violated the defendant's Fourth Amendment privacy interests, due in part, because of the massive amounts of private information contained on the phone).

[44] *See generally* California v. Greenwood, 486 U.S. 35 (1988) (finding there was no reasonable expectation of privacy protected by the Fourth Amendment for trash on public streets because the plaintiff voluntarily left the trash in a public area suited for public collection and thus did not have an objectively reasonable expectation of privacy).

[45] *See generally* United States v. Miller, 425 U.S. 435 (1976) (holding there was no reasonable expectation of privacy in a person's bank records because there is no legitimate expectation of privacy in information voluntarily conveyed to the bank).

[46] Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1059 (2019).

[47] *See* 15 U.S.C. § 6801–6809.

[48] *See* 45 C.F.R. § 164.500 (2020).

[49] *See* 20 U.S.C. § 1232g.

[50] Daniel J. Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ ("Tech companies are getting into health. Cable companies are providing Internet and phone. Various organizations perform functions of many different industries, such as schools, which perform financial services, health services, and so on.").

first such law was enacted in 2002.[51] By 2014, twenty-three states had introduced or considered data breach laws.[52] In the following years, the remaining states quickly enacted statutes. As of early 2018, Alabama became the last state to enact a data breach notification law.[53] Today, all fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information.[54] Part III will explore the difficulties that businesses of all sizes face when attempting to comply with the varying standards in these data breach statutes.[55]

While some commentators still consider the United States privacy regime to be inadequate,[56] some states are taking a proactive approach to protect individual rights.[57] States are gradually realizing the importance of data privacy laws and are beginning to implement more comprehensive privacy protections. For example, New Jersey has introduced the New Jersey Disclosure and Accountability Transparency Act (NJ DaTA), which establishes particular requirements for the disclosure and processing of personal information.[58] Furthermore, as of February 2022, twenty-two states have introduced comprehensive privacy bills, which are still pending at varying stages of the legislative process.[59]

---

[51] *Data Breach Notification Laws by State*, ITGOVERNANCE, https://www.itgovernanceusa.com/data-breach-notification-laws (last updated July 2018).

[52] *See 2014 Security Breach Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Dec. 23, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/2014-security-breach-legislation.aspx (listing the states that had proposed or finalized legislation on data breaches in 2014).

[53] *Data Breach Notification Laws by State*, *supra* note 51.

[54] *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[55] *See* discussion *infra* Part III.

[56] *See generally* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (arguing that a "simpler and more comprehensive approach to individual digital dignity is warranted . . ." in part because "[t]he United States lacks a single, comprehensive federal law that regulates the collection and use of personal information").

[57] *See generally* Chris Cwalina et al., *Nine States Pass New and Expanded Data Breach Notification Laws*, NORTON ROSE FULBRIGHT (June 27, 2019), https://www.dataprotectionreport.com/2019/06/nine-states-pass-new-and-expanded-data-breach-notification-laws/ (exploring recent state amendments to their data breach laws to include more encompassing privacy protections).

[58] Assemb. 3283, 219 Leg., Reg. Sess. (N.J. 2020).

[59] Taylor Kay Lively, *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PRO., https://iapp.org/resources/article/state-comparison-table/ (last updated Feb. 17, 2022).

The most comprehensive state legislation is likely California's recently enacted California Consumer Privacy Act of 2018 (CCPA), which went into effect at the beginning of 2020.[60] The CCPA focuses on the protection of individual rights by providing consumers with: (1) the right to know all data businesses collect about them;[61] (2) the right to request deletion of their data;[62] (3) the right to enforcement by the state Attorney General;[63] and (4) the right to a private action against companies that experience a data breach.[64] Some commentators consider the CCPA to be groundbreaking in the United States because it provides "consumers with unprecedented rights to access, protect, and delete data collected about them."[65] Other states offer fewer protections than California. Nevertheless, as mentioned above, legislation is rapidly expanding, and other states are expected to pass significant privacy laws.[66]

The sectoral approach to privacy at a federal level combined with the varying levels of protection offered from state to state make compliance challenging for businesses of all sizes. While support is increasing for a "comprehensive, national privacy law that would supersede and preempt state privacy laws," it will not likely happen for several years.[67] The United States may look to international standards for inspiration, such as the General Data Protection Regulation (GDPR)

---

[60] Bianca Karim, *Cause of Action for Breach of Data Security for Consumers' Information*, 85 CAUSES OF ACTION 2d 635 (2020).

[61] CAL. CIV. CODE § 1798.100(a) (West 2020) ("A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.").

[62] *Id.* § 1798.105(a) ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.").

[63] *Id.* § 1798.155(b) ("The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.").

[64] *Id.* § 1798.150(a)(1) ("Any consumer whose nonencrypted and nonredacted personal information, as defined [within] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action[.]").

[65] Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collaterizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 CATH. U.J.L. & TECH. 187, 223 (2018).

[66] *Data Protection Laws of the World*, DLA PIPER, https://www.dlapiperdataprotection.com/?t=law&c=US (last modified Jan. 24, 2022).

[67] *Id.*

in the European Union,[68] which has broader applicability and prioritizes the protection of individual rights.[69] Without an omnibus approach, the current system of privacy protection in the United States makes compliance difficult for good faith businesses that prioritize data security and leaves data subjects unprotected.

III. THE UNFEASIBLE MISSION OF COMPLYING WITH FIFTY DIFFERENT STATE STATUTES

Companies that do business in multiple states may find it difficult, if not impossible, to comply with the different requirements included in the data breach regulations across fifty states. This Part will highlight some of the difficulties that businesses of all sizes face under the United States' current patchwork privacy regime. Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data or information brokers, government entities, etc.);[70] how to define "personal information" (e.g., name combined with SSN, driver's license, state ID, account numbers, etc.);[71] what constitutes a breach (e.g., unauthorized acquisition of data);[72] what are the requirements for notice (e.g., timing or method of notice, who must be notified);[73] and what exemptions are available (e.g., for encrypted

[68] Karim, *supra* note 60.

[69] Barrett, *supra* note 46, at 1060.

[70] *See, e.g.*, ALA. CODE § 8-38-2(2) (2018) (defining a covered entity as "[a] person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information"); W. VA. CODE § 46A-2A-101(2) (2008), ("'Entity' includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit.").

[71] *See, e.g.*, S.C. CODE ANN. § 39-1-90(D)(3) (2021) (defining personal identifying information as "the first name or first initial and last name in combination with . . . social security number; driver's license number . . . financial account number, or credit card [number] . . . other numbers or information which may be used to access a person's financial accounts . . ." but "does not include information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records"); N.D. CENT. CODE § 51-30-01(4)(a) (2021) (including information such as date of birth and mother's maiden name).

[72] *See, e.g.*, N.D. CENT. CODE § 51-30-01(1) (2021) ("'Breach of the security system' means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable."); FLA. STAT. § 501.171(1)(a) (2021)("'[B]reach' means unauthorized access of data in electronic form containing personal information.").

[73] *See, e.g.*, N.D. CENT. CODE § 51-30-02 (requiring notice to attorney general and consumers); *id.* § 51-30-05 (requiring either written notice, electronic notice, or substitute notice, which includes email, posting on company website, or notice to major

information or publicly available information).[74] Some of these definitions overlap from state to state; however, even these basic provisions may have differences in their construction and language making it a headache for businesses to comply with each one.

For example, every state's statutes cover financial information, such as credit card numbers, along with any passwords associated with that information.[75] Yet, just four states' statutes protect biometric data, including things like fingerprints and retina images.[76] Only one of those states extends the protections to DNA.[77] While most states consider email and password sensitive information, California and Florida do not cover "your mother's maiden name, which is often used as a security question."[78] Furthermore, most states have a provision that the notification requirement is only triggered if stolen personal information is unencrypted data or if the encryption key is also stolen.[79] Thus, merely knowing when a breach is significant or personal enough to trigger a warning can be complicated.

Another example that illustrates the difficulties that a good faith business may encounter when attempting to comply with all fifty states' laws is the notification timelines required from state to state. Once a company has gone through the process described above to identify if

statewide media). *But see* W. VA. CODE § 46A-2A-102 (2008) (declining to incorporate any notification requirement to the attorney general).

74 *See, e.g.*, FLA. STAT. § 501.171(1)(g)(2) (2021) ("The term [personal information] does not include . . . information that is encrypted"); WASH. REV. CODE § 42.56.590(11) (2021) (Washington excludes an exception for "secured" information. "'[S]ecured' means encrypted in a manner that meets or exceeds the national institute of standards and technology standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.").

75 Michael Keller, *Holiday Shopping? How Much Do Data Breach Notification Laws Protect?*, ALJAZEERA AM. (Dec. 1, 2014, 5:00 AM), http://america.aljazeera.com/multimedia/2014/12/to-catch-a-breachhowmuchdodatabreachnotificationlawsprotect.html.

76 *Id.*

77 *Id.*

78 *Id.*

79 *See, e.g.*, ALASKA STAT. ANN. § 45.48.090(7) (West 2020) ("'[P]ersonal information' means information in any form on an individual that is not encrypted or redacted, or is *encrypted* and the encryption key has been accessed or acquired") (emphasis added); ARIZ. REV. STAT. ANN. § 18-552(C) (2021) ("A person that maintains *unencrypted* and *unredacted* computerized personal information that the person does not own or license shall notify, as soon as practicable, the owner or licensee of the information on discovering any security system breach . . . .") (emphasis added); ARK. CODE ANN. § 4-110-105(a)(1) (2021) ("Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose *unencrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person.") (emphasis added).

personal information was compromised and which statute(s) may be implicated, they must then recognize how quickly they need to notify the affected data subjects. Timelines can range from "immediately following discovery [of the breach]"[80] or "in the most expeditious time possible and without unreasonable delay"[81] to "not later than ninety days after the discovery of [the] breach[.]"[82]

Furthermore, some states add additional requirements such as "within 45 days . . . [after a] determination that a breach has occurred *and* is reasonably likely to cause substantial harm . . . ."[83] Additionally, several states require that the notifications be made to the Attorney General,[84] while others put conditions on the Attorney General notification[85] or forego that requirement altogether.[86] All of these conflicting requirements inevitably confuse companies who do business in multiple states, resulting in inadequate compliance and impacting some data subjects as a result.[87] A more comprehensive, uniform standard would make compliance with notification timelines more attainable.

While no state has passed legislation comparable to the CCPA, there are promising legislative trends focused on providing consumer protection and creating "norms" across the entire United States.[88] These norms may make compliance slightly less complicated. The legislative trends include amendments that have: (1) expanded definitions of "personal information" (e.g., to include biometric information, email

80 MONT. CODE ANN. § 30-14-1704(2) (2021).

81 ALASKA STAT. ANN. § 45.48.010(b).

82 CONN. GEN. STAT. § 36a-701b(b)(1) (2021).

83 ALA. CODE § 8-38-5(b) (2018) (emphasis added).

84 *See, e.g.*, MD. CODE ANN. COM. LAW § 14-3504(h) (West 2019) ("[A] business shall provide notice of a breach of the security of a system to the Office of the Attorney General.").

85 *See, e.g.*, N.D. CENT. CODE § 51-30-02 (2021) ("In addition, any person that experiences a breach of the security system as provided in this section shall disclose to the attorney general by mail or electronic mail any breach of the security system which *exceeds two hundred fifty individuals*.") (emphasis added).

86 *See, e.g.*, OHIO REV. CODE ANN. §§ 1347.12 (West 2015) (omitting any attorney general notification requirement).

87 Luke Irwin, *Data Breach Notification Requirements*, IT GOVERNANCE USA BLOG (Dec. 16, 2019), https://www.itgovernanceusa.com/blog/when-should-an-organization-report-a-data-breach ("Organizations that conduct business across all 50 states therefore have a considerable compliance challenge.").

88 *See 2020 Security Breach Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Nov. 4, 2020) https://www.ncsl.org/research/telecommunications-and-information-technology/2020-security-breach-legislation637299951.aspx.

address with a password, passport number, etc.);[89] (2) reduced the time window within which businesses must report a breach;[90] (3) required reporting of breaches to the state attorney general;[91] and (4) provided for free credit freezes or identity theft protection for victims of data breaches.[92] These trends are a step in the right direction to raise the privacy protections afforded to data subjects in the United States.

Despite these trends, the fact that each state has a unique statute makes compliance tricky, if not nearly impossible, for businesses of all sizes. Certainly, the trends are narrowing the gaps between the state laws. A uniform federal solution would minimize the compliance problem by providing businesses of all sizes with one set of proper rules.

IV. THE PATCHWORK PRIVATE RIGHT OF ACTION PROVIDED TO PEOPLE ACROSS THE UNITED STATES

On the other end of the data breach is the affected data subject. In addition to the business challenges described above, data subjects are not adequately protected by existing legal remedies. This Part will briefly discuss the current landscape of private actions afforded to data subjects once their data has been breached. Generally, a private right of action allows injured parties to sue on their behalf for damages caused by another's violation of federal or state statutes, rather than rely on

---

89 *See, e.g.*, Chris Cwalina et al., *Nine States Pass New and Expanded Data Breach Notification Laws*, NORTON ROSE FULBRIGHT (June 27, 2019), https://www.dataprotectionreport.com/2019/06/nine-states-pass-new-and-expanded-data-breach-notification-laws/ (analyzing Washington H.B. 1071, which expanded the definition of personal information "to include the following categories: birthdate; unique private keys for signing electronic records; student, military, or password identification numbers; medical information; biometric information; and online login credentials"); *id.* ("New Jersey's law expands the definition of 'personal information' to include usernames, email addresses, passwords, and security questions and answers affiliated with an individual's online account.").

90 *See, e.g.*, S.H.B. 1071, 2019 AMS WM S3925.1 (Wash. 2019) (shortening the notification timeline from forty-five days to "thirty calendar days after the breach was discovered").

91 *See* BAKERHOSTETLER, DATA BREACH CHARTS 16 (2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (referencing Arizona's data breach law "[e]ffective Aug. 1, 2018, if the breach requires notification of more than 1,000 individuals, notification must be made to the attorney general and the three largest nationwide consumer reporting agencies").

92 *See, e.g.*, H.B. 4806, 190th Gen. Assemb., Reg. Sess. (Mass. 2018) ("If a person . . . experienced a[] [qualified breach] . . . and such breach of security includes a social security number, the person shall contract with a third party to offer to each resident . . . credit monitoring services at no cost to said resident . . . .").

public enforcement by authorities who may be unable—or unwilling—to bring cases for the benefit of a single individual.[93]

As a threshold matter, in the wake of a data breach, merely finding a right of action can be quite difficult.[94] The general theories of recovery range from common law causes of action (including negligence, breach of contract, and unjust enrichment) to remedies derived from state and federal statutes (including data breach notification and unfair and deceptive trade practice statutes).[95] Ultimately, there is no clear path forward for recovery post-data breach. Recent attempts to fit data privacy within existing rights have met strong court resistance.[96] As a result, "creative new theories offer attractive instruments for redress."[97] Nonetheless, these theories face significant challenges, starting with identifying a legally enforceable right of action.[98]

After a large data breach, consumers from multiple states may be affected, and a class action suit may be initiated. Class actions are often considered because it would be inefficient for individuals to bring claims due to the limited amount they can recover.[99] When faced with a class-action lawsuit, courts will often analyze claims under various states' data breach notification statutes—potentially, even all fifty state statutes. When it comes to a private right of action, courts categorize the statutes in one of four ways: (1) statutes that expressly provide a private right of action;[100] (2) statutes that contain an explicit attorney general enforcement clause;[101] (3) statutes that are ambiguous or

93 *See* William E. Kovacic, *British Institution of International & Comparative Law Third Annual Conference on International and Comparative Competition Law: The Transatlantic Antitrust Dialogue*, FED. TRADE COMM'N (May 15, 2003), https://www.ftc.gov/public-statements/2003/05/private-participation-enforcement-public-competition-laws ("Private rights of action diminish, if not eliminate, the gate-keeping authority of public prosecutors and reduce their ability to control the development of policy by their selection of cases. Specifically, independent private rights to prosecute deny prosecutors the capacity to modulate the law's application by deciding to prosecute some violations more aggressively and prosecute other offenses less vigorously.").

94 *See* Justin H. Dion & Nicholas M. Smith, *Consumer Protection—Exploring Private Causes of Action for Victims of Data Breaches*, 41 W. NEW ENG. L. REV. 253, 268–70 (2019) (describing the lack of a private right of action under federal statutes such as the HIPAA, GLBA, COPRA, and FTCA acts).

95 Karim, *supra* note 60, §§ 4–7.

96 Reidenberg, *supra* note 38, at 877.

97 *Id.* at 890.

98 *Id.*

99 *See* 140 AM. JUR. TRIALS 327 § 8 (2015).

100 *See, e.g.*, CAL. CIV. CODE § 1798.150(a)(1) (West 2020); MD. CODE ANN., COM. LAW §§ 14-3508 (West 2008).

101 *See, e.g.*, ARK. CODE ANN § 4-110-101 (2005) (providing that a "violation of this chapter is punishable by action of the Attorney General under the provisions of § 4-88-

provide non-exclusive remedy clauses;[102] and (4) statues that are silent to the matter.[103] Citizens in states that provide a right of action can clear the first hurdle but may face other issues, as discussed below.

On the other end of the spectrum, some states do not expressly provide a private right of action. Resultingly, data subjects living in these states may face an immediate obstacle in their attempt to recover for any harm suffered. While these statutes generally do not explicitly preclude a private action, courts have interpreted certain provisions in the statute to deny an avenue of recovery.[104] Courts have interpreted statutes that contain an explicit attorney general enforcement clause to close the door on a private right of action from a data breach notification standpoint.[105] Courts have interpreted both permissive clauses (i.e., "the AG may . . .")[106] and mandatory language (i.e., "the AG shall . . .")[107] to deny a private right of action and dismiss these claims at the pleading stage.

Various statutes that include explicit attorney general enforcement provisions also include non-exclusive remedy provisions.[108] If the statute provides a non-exclusivity clause, courts will generally find that this creates ambiguity as to whether a private right of action exists and

101 et seq."); IDAHO CODE ANN. § 28-51-107 (West 2006) ("[T]he primary regulator may bring a civil action to enforce compliance" with the state's data-breach notice statute.); MASS. GEN. LAWS ch. 93H, § 6 (2007) (stating that the "attorney general may bring an action . . . to remedy violations of this chapter"); NEB. REV. STAT. § 87-806 (2018) (providing that "the Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of" the data-breach notice statute).

102 *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014) (classifying claims brought under Colorado, Delaware, Iowa, Kansas, Michigan, and Wyoming statutes to be considered to have "[a]mbiguous language or non-exclusive remedies").

103 *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1341 (N.D. Ga. 2019) (analyzing Wisconsin's data breach notification law and determining that it is silent as to the question of whether a private right of action exists).

104 *Target Corp.*, 66 F. Supp. 3d at 1168–69.

105 *Id.*

106 *Id.* ("Texas's data-breach notice statute provides *only* for attorney general enforcement, stating repeatedly that '[t]he attorney general *may* bring an action to recover the civil penalt[-y, -ies] imposed under this subsection . . . .'") (emphasis added).

107 *Id.* at 1168 (dismissing a private claim at the pleadings stage under Connecticut's data breach notification provision which states, "violations of the statute 'shall be enforced by the Attorney General'" because the language "clearly limits enforcement power to the state's attorney general" exclusively); *Equifax Inc.*, 362 F. Supp. 3d at 1340 (dismissing the Connecticut plaintiffs' claims because the statutory language "explicitly limits enforcement to the Attorney General").

108 *Target Corp.*, 66 F. Supp. 3d at 1169 (classifying claims brought under Colorado, Delaware, Iowa, Kansas, Michigan, and Wyoming statutes to be considered to have "[a]mbiguous language or non-exclusive remedies").

will not dismiss these claims at the pleadings stage.[109] Though, if the statute includes both an attorney general enforcement clause and a nonexclusive remedy provision, courts may still deny a private right of action to the data subject.[110] Since many states do not include nonexclusive remedy provisions, an affected consumer in these states will have to rely on other public enforcement procedures in their respective states.[111]

Unfortunately, these public enforcement mechanisms are often inadequate or selective. A contributing factor to this is the lack of defined statutory rights surrounding data breaches which, in turn, creates ineffective public enforcement mechanisms.[112] For example, the Federal Trade Commission (FTC) can assert claims through the FTC's "'unfair and deceptive trade practice' jurisdiction."[113] Companies may violate a state's unfair and deceptive trade practice laws when they "inaccurately describe their information handling practices."[114] The prosecution for deceptive trade practices is generally focused on curbing the company's deceptive practices, not on compensating the victim for any harm they suffered.[115]

Inadequate focus on stopping harmful conduct can result in companies abusing the system. Perhaps, a large company may decide to pay a fine for violating the statute rather than notify the customers and risk greater loss from a damaged reputation.[116] For example, Arizona's statute, which is enforceable only by the state attorney general, allows data subjects to bring an action, but caps the civil penalty at $5,000.[117]

---

109 *See id.* (declining to dismiss plaintiffs' Colorado claim because "Colorado's data-breach notice statute provides that the 'attorney general may bring an action . . . to address violations of this section,' but also provides that the 'provisions of this section are not exclusive.'"); *id.* (declining to dismiss Delaware claims because the nonexclusive remedy provisions indicate that "it is at least ambiguous whether there is a private right of action").

110 *Equifax Inc.*, 362 F. Supp. 3d at 1339–40 (analyzing the attorney general enforcement provision in conjunction with the nonexclusive remedy provision which states, "'the remedies provided by this section shall be in addition to any other lawful remedy available'" but ultimately concluding that a conflicting provision in the statute which states, "'the provisions of this section shall be exclusive and shall preempt any provisions of local law . . . and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section'" to preclude against a private right of action despite the nonexclusive remedy provision).

111 *See* Reidenberg, *supra* note 38, at 885.

112 *Id.*

113 *Id.* at 885–86.

114 *Id.*

115 *Id.* at 886.

116 *See id.* ("A company risks liability by making a disclosure, but does not risk accountability by remaining silent.").

117 ARIZ. REV. STAT. ANN. § 44-7601 (2006).

For large corporations, the costs associated with data security can be in the hundreds of millions of dollars.[118] Thus, the companies who have the most data about consumers may be better off foregoing the costs associated with preventing breaches and simply paying the penalty, if they are caught.

This is just one example of how existing public enforcement mechanisms can be abused, which can lead to inadequate protection of data subjects. It follows that under the current landscape, consumers may be forced to bear the costs of a data breach. Instead, companies should be held accountable via a private right of action, thereby shifting the cost of a data breach onto the company itself. Accountability will inspire companies to invest into their data security practices in fear of large class action settlements from a data breach. In turn, the market, overall, will become more secure and the breach frequency should decrease, thereby exposing data subjects to less harm.

The issues presented in this Part highlight one major roadblock and the consequences that the minor differences in statutory language have created, which exacerbate the need for a federal solution to protect data subjects more adequately. Predominantly, the goal should be to limit the number of breaches, increase data security, and reduce the risk to consumers. Allowing companies to cut corners will continue to expose data subjects to unnecessary risks. A federal privacy regulation should take both the businesses' and consumers' goals into account to provide a comprehensive scheme to protect both sides.

V. A PROPOSED FEDERAL SOLUTION

The amount of data breached has risen steadily since 2005.[119] It is estimated that a business will fall victim to a ransomware attack every two seconds by 2031.[120] As this problem continues to rapidly expand, the urgency of a federal solution is mounting. This Part will examine a proposed solution to address the two main issues discussed above, i.e., providing a private right of action to affected data subjects and establishing uniform guidelines for businesses to follow.[121] By

---

118 Steve Morgan, *Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017–2021*, CYBERCRIME MAG. (June 10, 2019), https://cybersecurityventures.com/cybersecurity-market-report/ ("Jamie Dimon, chairman and CEO at J.P. Morgan Chase & Co. . . . states that the financial services giant spends roughly $600 million each year on cybersecurity[.]").

119 Daniel Funke, *By the Numbers: How Common Are Data Breaches—and What Can You Do About Them?*, POLITIFACT (Sept. 23, 2019), https://www.politifact.com/article/2019/sep/23/numbers-how-common-are-data-breaches-and-what-can-/.

120 Cook, *supra* note 17.

121 *See* discussion *supra* Parts III–IV.

addressing these two main issues, a federal privacy regulation can shift the cost of data breaches to the business sector, which is more apt to shoulder the cost via a private right of action. Once the business bears the burden, it will be more incentivized to increase its security measures accordingly as per a set of proposed uniform guidelines. In theory, this will decrease the breach frequency and lower the overall "cost" of data breaches as a whole.

First, when it comes to the private right of action, establishing a federal regulation with a private right of action will incentivize companies to comply with defined procedures and protect consumers if their data is inevitably breached. Under the current landscape, "[t]he real search behind the efforts to remedy privacy violations is a search to create new legal rights."[122] For now, the movement for privacy enforcement continues to expand in search of a proper remedy to disrupt the current scheme that protects the privacy violators.[123] This must be addressed in any federal approach.

Currently, without federally defined statutory rights, companies are not held legally accountable, and there is a lack of liability for improper treatment of personal information in the private business world.[124] Large data breaches highlight potential issues with the current scheme and bring those issues into the public spotlight and "provide[] an incentive for legislative action to establish greater legal certainty for the treatment of personal information."[125] There have been recent attempts to address the existing statutory gaps using federal legislation.[126] For example, former Attorney General Eric Holder has advocated for a federal standard to "simplify" and "strengthen" consumer protections.[127] Additionally, members of Congress have already attempted to propose several data breach laws, but for various reasons, they have not provided adequate protection to those whom

122 Reidenberg, *supra* note 3838, at 898.

123 *Id.*

124 *Id.*

125 *Id.*

126 *See, e.g.*, Michael D. Simpson, Comment, *All Your Data Are Belong to Us: Consumer Data Breach Rights and*

Remedies in an Electronic Exchange Economy, 87 U. COLO. L. REV. 669, 688 (2016) (footnotes omitted) ("For example, bills introduced during the 113th Congress included the Personal Data Protection and Breach Accountability Act of 2014, which would have imposed personal data privacy and security requirements on interstate businesses and created both public and private rights of action for violations.").

127 Keller, *supra* note 75.

"these laws are supposed to protect."[128] As the debates rage on, ordinary people remain exposed and vulnerable without sufficient options to recover under the existing scheme.[129] Action must be taken sooner rather than later to curtail this exposure and protect the United States citizens.

Some attorney generals have expressed concerns about a national system.[130] For example, Connecticut Attorney General George Jepsen has concerns that a federal solution "could reduce the number and effectiveness of regulators at the state level who fight data breaches."[131] Additionally, Maryland Attorney General Douglas Gansler stated a valid concern that a federal regulation "should not preempt state enforcement. Any federal standards should be a floor, not a ceiling, allowing states to enact stricter standards."[132] Conversely, some commentators believe California's strict new protections are the reason for the lack of a federal solution.[133]

The argument that the national law should create a floor is enticing; however, it does not address the difficulties that businesses will face in complying with different state regulations. If the federal rule is simply a floor, each state would still be free to enact stricter laws which may eventually lead back into the patchwork privacy problem that we are currently facing. Furthermore, the longer we wait to set a national standard, the more exposed data subjects may be in states with lesser protections. By setting a baseline for security measures that businesses must comply with, the overall security of the private sector will be increased, and thus, the frequency of data breaches should decline.

Consequently, the United States should revamp the current privacy regime entirely and take into account both issues described above. At the forefront, there must be a private right of action to allow consumers a path to recovery and hold businesses accountable. Furthermore, there must be defined reasonable security measures, whether included in the

128 Drew Mitnick, *No More Waiting: It's Time for a Federal Data Breach Law in the U.S.*, ACCESSNOW (Apr. 10, 2018, 10:51 AM), https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/.

129 *Id.*

130 Tod Newcombe, *States Approach Federal Data Breach Law with Caution*, GOVERNING (Sept. 18, 2014), https://www.governing.com/archive/gov-federal-cybersecurity-law.html.

131 *Id.*

132 *Id.*

133 Daniel Castro & Ashley Johnson, *Why Can't Congress Pass Federal Dave Privacy Legislation? Blame California*, INFO. TECH. & INNOVATION FOUND.: INNOVATION FILES (Dec. 13, 2019), https://itif.org/publications/2019/12/13/why-cant-congress-pass-federal-data-privacy-legislation-blame-california.

statute itself or accompanying regulations, that guide good-faith businesses to raise the security of the industry entirely.

A. *Including a Private Right of Action for Data Subjects Whose Information is Breached*

First and foremost, any federal solution should include a private right of action. Private rights of action have worked in other industries to incentivize corporations to strengthen their internal processes and invest in safeguards to minimize potential lawsuits and thus protect consumers.[134] Civil litigation has made dangerous machines safer, improved product safety through tort law, and improved the safety of motor vehicles.[135] None of this would have been possible had these industries been regulated by inadequate and underfunded regulatory regimes akin to the current patchwork privacy framework.[136] Private rights of action can "'catalyz[e] a societal shift toward a thicker notion of industrial responsibility,' as it did with mass environmental torts and product liability."[137] Private claims bring adverse publicity and expose industry practices that may provoke productive "industry-wide changes."[138] To date, any changes that have occurred in the privacy world still fall short.[139]

The federal solution must be careful not to weaken existing protections offered to customers via the various statutes.[140] Any new federal standard must not prevent states from adding protections. A federal data breach law should not create a ceiling preventing more strict state enforcement but should create a baseline that states can build upon;[141] although the floor should be high enough to protect most citizens adequately and to avoid falling back into the same abyss we are in. Perhaps the federal solution can find inspiration from the CCPA to create a privacy framework that mandates companies to take

134 Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 831 (2020).

135 *Id.*

136 *Id.*

137 *Id.* at 832 (alteration in original) (quoting Julie E. Cohen, *Information Privacy Litigation as a Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 574 (2017)).

138 Reidenberg, *supra* note 38, at 898.

139 *Id.*

140 G.S. Hans, *White House Data Breach Legislation Must be Augmented to Improve Consumer Protection*, CTR. FOR DEMOCRACY & TECH. (Jan. 16, 2015), https://cdt.org/insights/white-house-data-breach-legislation-must-be-augmented-to-improve-consumer-protection/.

141 Mitnick, *supra* note 128.

reasonable security measures to protect personal information.[142] This would provide a baseline that the legislature can build upon as the digital universe continues to expand.

Still, a federal solution may need to build upon the framework of the CCPA. The CCPA provides that a "consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain *reasonable security procedures* . . . may institute a civil action[.]"[143] Though, the CCPA does not define what reasonable security measures would entail.[144] This leaves businesses open to potentially crippling liability if they fall below the ambiguous definition of "reasonable security procedures."

Under the CCPA, if a litigant can bring a private right of action as described above, they may "recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."[145] Thus, if a business has only 100,000 records compromised (a relatively small amount in the world of big business), it could potentially be liable for up to $75,000,000 resulting from a class-action lawsuit. Due to the theoretically massive settlements coupled with a vague definition of reasonable security measures, a private right of action will likely open a large stream of litigation. A federal solution must take this into account and provide businesses of all sizes with a more detailed roadmap of what constitutes reasonable security measures. By doing so, it would accomplish several key goals: (1) ensuring the customer data is more secure by incentivizing businesses to implement up-to-date security measures; (2) allowing businesses to protect themselves from potentially crippling liability by complying with delineated security measures; (3) reduce the burden on the courts; and (4) provide consumers a clearer path to recovery if businesses fail to comply.

---

142 CAL. CIV. CODE § 1798.150(a)(1) (West 2018) ("Any consumer whose nonencrypted and nonredacted personal information, as defined [within] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain *reasonable security procedures* and practices appropriate to the nature of the information to protect the personal information may institute a civil action[.]") (emphasis added).

143 *Id.* (emphasis added).

144 IAN C. BALLON, *Litigation Risks and Compliance Obligations Under the California Consumer Privacy Act*, *in* E-COMMERCE AND INTERNET LAW 26-400, 26-425 (2019).

145 CAL. CIV. CODE § 1798.150(a)(1)(A).

B. *Simplifying the Requirements to Make Compliance Attainable*

Next, a federal solution must consider the needs of the businesses that will need to comply with the law. One major factor which currently plagues these businesses under the existing patchwork approach is the lack of standards outlining what actions they can take to adequately protect consumer information (and thus comply with the law). Any federal solution should look to define a floor of protections that will allow good-faith businesses to enact security procedures designed to protect both data subjects from a breach and the business itself from liability. This can be done by defining "reasonable security measures" either in the statute or accompanying regulations.

Some "sectors" have already delineated what is considered a "reasonable security measure."[146] If the United States chose to implement a federal data breach/privacy regulation, it could build upon these existing laws. A proposed federal solution could model reasonable safety measures after the GLBA's Safeguards Rule. While the GLBA applies solely to financial institutions, several concepts can be expanded into the framework of a data breach statute. The GLBA outlines reasonable security measures, which in turn incentivize financial institutions to increase their data protection strategies, thereby increasing security and decreasing potential breaches.[147] Under the GLBA, the precautions that businesses must take to be considered "reasonable" can be broken down into three categories: (1) employee management and training safeguards;[148] (2) information systems safeguards;[149] and (3) detecting and managing systems safeguards.[150]

[146] For examples of several sectors delineating the security measures, see 16 C.F.R. § 314.4 (2021) for the GLBA safeguards rule and 45 C.F.R. § 164.306 (2021) for the HIPAA security rule.

[147] *See* Stephen E. Breidenbach & Terese L. Arenth, *Navigating the Ambiguous Requirement of 'Reasonable Security' Measures While Protecting Personal Information*, N.Y. L.J. (May 8, 2020, 2:10 PM), https://www.law.com/newyorklawjournal/2020/05/08/navigating-the-ambiguous-requirement-of-reasonable-security-measures-while-protecting-personal-information/ ("As most businesses collect and maintain sensitive personal information about their customers, the key takeaway is to first assess the type of business that you operate and the types of personal information that you collect. From that starting point, develop, implement and maintain a sound security plan to collect only the information that you need, to keep that information safe, and to dispose of it securely. This will form the foundation to help your business meet its legal obligations and protect that sensitive data.").

[148] 16 C.F.R. § 314.4(b)(1) (2021).

[149] *Id.* § 314.4(b)(2).

[150] *Id.* § 314.4(b)(3).

First, the category of employee management and training safeguards refers to developing programs to ensure that employees adopt good security practices, such as basic requirements like strong computer passwords, which are updated regularly.[151] The FTC guidelines delineate several specific examples to consider, including: (1) background checks when hiring employees;[152] (2) "limiting access to customer information to employees who have a business reason to see it";[153] (3) "training employees on the basic steps to maintain security, confidentiality, and integrity";[154] (4) "developing policies for employees who telecommute"; (5) "imposing disciplinary measures for security policy violations";[155] (6) "preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names";[156] and (7) "tak[ing] steps to ensure the secure transmission of customer information."[157] These are several of the delineated measures in the FTC regulations for the GLBA, but this is not an exhaustive list of the types of safeguards that financial institutions may want to consider.[158]

Second, the GLBA outlines several key information systems safeguards that companies should consider. According to § 314.4(b)(2), "information systems include network and software design, as well as information processing, storage, transmission, [retrieval,] and disposal."[159] As per the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, established by the Department of the Treasury, the final guidelines require "an institution to consider the need for access controls in light of the institution's various customer information systems and adopt such controls as appropriate."[160] Some of these measures are quite simple, such as storing records in a room or cabinet that is locked when unattended, while some are more cumbersome, such as ensuring that storage areas are protected against

151 *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

152 *Id.*

153 *Id.*

154 *Id.*

155 *Id.*

156 *Id.*

157 *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, *supra* note 151.

158 *Id.*

159 16 C.F.R. § 314.4(b)(2) (2021).

160 *See* Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616, 8622 (Feb. 1, 2001) (to be codified at 12 C.F.R. pt. 30).

destruction or damage from physical hazards like fires or floods. One of the most important aspects of information security is the assurance of secure transmission of customer information. The FTC recommends that "when [covered institutions] transmit credit card information or other sensitive financial data," they should use a "secure connection, so that the information is protected in transit."[161] If financial institutions transmit sensitive data by email over the Internet, the information should be encrypted to reduce the possibility of data theft.[162] Again, these regulations delineate guide rails for institutions, which can be flexible depending on the business size and needs.[163]

Finally, detecting and managing systems safeguards are intended to prevent hacks or system-wide failures. According to the FTC, typical safeguards that a company could put in place include, but are not limited to: (1) "keep[ing] logs of activity on [the] network and monitor[ing] them for signs of unauthorized access to customer information";[164] (2) "us[ing] an up-to-date intrusion detection system";[165] (3) "monitor[ing] both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from [the] system to an unknown user";[166] and (4) "insert[ing] a dummy account into each of [the] customer lists and monitor[ing] the account to detect any unauthorized contacts or charges."[167] The FTC Safeguard Rules encourage financial institutions to look to industry standards and best practices.[168]

Perhaps a federal data breach solution could define a baseline of reasonable security measures similar to the scheme in the GLBA to achieve the goal of protecting the entire business storage system. By detailing what "reasonable security measures" entails, the legislation

161 *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, *supra* note 151.

162 *Id.*

163 *Id.*; Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. at 8628 ("The Board believes that the compliance burden is minimized for small institutions because the Guidelines expressly allow institutions to develop security measures that are 'appropriate to the size and complexity of the [institution]'.").

164 *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, *supra* note 151.

165 *Id.*

166 *Id.*

167 *Id.*

168 *See* Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484, 36,488 (May 23, 2002) (to be codified at 16 C.F.R. pt. 314) (stating that a business should adopt "a program that has a continuous life cycle designed to meet the needs of a particular organization or industry").

will guide good-faith businesses. In turn, those businesses will be able to improve their security systems or be subject to liability for failing to take reasonable action. As a result, this will improve the entire data security landscape, reduce the number of breaches, lower the burden on the court system, and protect data subjects.

At first glance, it may seem that this would increase the costs to the business as they will have to implement these "reasonable security measures." Though, the costs will likely pale in comparison to the potentially crippling class action suits that can be brought for a violation of a statute like the CCPA.[169] Under the current regime, the customers bear the brunt of the costs associated with breaches. It is time that a federal statute is enacted, allowing for a private right of action to shift those costs to the businesses that are more equipped to handle the expenses. Businesses will bear upfront costs to enact reasonable security measures.[170] Some estimate that these costs can rise upwards of two million dollars for companies with more than five hundred employees.[171] But these investments will lead to increased security and data will be breached less frequently. If a business can prevent a single breach, it can save millions of dollars.[172] Therefore, companies can cut costs in the long run by investing in data security in the short term. For any remaining risk, companies can invest in cyber insurance to protect themselves in the event of a breach. The cyber insurance market is growing and is expected to be a 28.6-billion-dollar industry by 2026.[173] This helps spread the risk to the entire online industry and minimizes the risk of catastrophic consequences to a single business.[174] In turn, the business sector is more protected while achieving the end goal of protecting the consumer's information and privacy.

---

169 *See* discussion *supra* Section V.A.

170 Nicole Lindsey, *New Report Suggests Initial Compliance Costs for CCPA Could Reach $55 Billion*, CPO MAG. (Oct. 15, 2019), https://www.cpomagazine.com/data-protection/new-report-suggests-initial-compliance-costs-for-ccpa-could-reach-55-billion/ (stating that "small companies with less than 20 employees . . . are projected to average around $50,000 [in compliance costs] . . . [a]t the top end of the range are companies with more than 500 employees ($2 million or more in initial CCPA compliance costs)").

171 *Id.*

172 *See* discussion *supra* Section V.A.

173 *Cyber Insurance – H1, 2020 Market Highlights*, COWBELL CYBER (June 22, 2020), https://cowbell.insure/2020/06/22/cyber-insurance-h1-2020-market-highlights/.

174 *Insurance 101*, INS. INFO. INST., https://www.iii.org/article/insurance-101 (last visited Nov. 5, 2020) (stating that the central concept of insurance is to divide risk "among many members of a group, then [the risks] need fall but lightly on any single member of the group. Thus, misfortunes that could be crushing to one can be made bearable for all. Viewed as a form of mutual aid, risk-sharing can be seen not only as sound business practice, but as enlightened social behavior rooted in accepted principles of ethics.").

The need for a federal solution to data privacy is mounting. As sensitive and personal data is shared more rapidly than ever before, Congress must take action to protect it. The goal of a federal privacy regime should be to minimize the number of breaches that occur. In turn, this will decrease the "cost" caused by data breaches. To achieve this goal, the federal solution should provide businesses with a more robust set of security guidelines. This will improve the privacy protections afforded to data subjects immediately through increased security measures in the market. Furthermore, the solution should provide a private right of action to data subjects exposed in a breach that results from a business not following those reasonable measures. This will further incentivize businesses to invest in data privacy and security in the short term, further strengthening the security measures in the market. Any federal solution should keep these two fundamental principles in mind to achieve the end goal of decreasing data breaches in the long run.

VI. CONCLUSION

As data breaches continue to become prevalent, a federal solution is more important now than ever. The current patchwork regime is too complicated for businesses to comply with, which results in inadequate protection of consumers' privacy interests. The current model is a reactive approach centering around notification only after the breach has occurred and the damage has largely been inflicted. At our current trajectory, it is not a matter of if the data will be stolen, but when. The United States should opt to take a proactive approach to protect its citizens and uphold their privacy interests. It is uncertain if a federal solution will be implemented soon. If not, the citizens remain vulnerable and are forced to shoulder the costs of a data breach. A federal solution should implement a baseline floor for businesses across the country to comply with. Furthermore, it should provide a private right of action if businesses do not meet that floor. This will incentivize businesses to invest in reasonable security measures, which will decrease the breach frequency and shift the costs of data privacy off of the shoulders of the citizens and on to the business sector which is more apt to shoulder the expense.