Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 14 | Issue 2 Article 8

6-22-2020

SAVING SMALL BUSINESS FROM THE BIG IMPACT OF DATA BREACH: A TIERED FEDERAL APPROACH TO DATA PROTECTION LAW

Nadia Udeshi

SAVING SMALL BUSINESS FROM THE BIG IMPACT OF DATA BREACH: A TIERED FEDERAL APPROACH TO DATA PROTECTION LAW

ABSTRACT

Small businesses provide a significant positive impact on the American economy. However, the current fragmented federal and state data protection and breach notification legal scheme puts the viability of small businesses at risk. While the probability of data breaches occurring continues to increase, small businesses lack the financial and technological resources to contend with the various state and federal laws that impose different monetary penalties and remedial requirements in the event of such breaches. To preserve the viability of small businesses, Congress should enact a centralized, multi-tiered federal data protection and breach notification framework that preempts state laws, imposes minimum cybersecurity standards, and in the event of a data breach, delineates penalties and remediation requirements. Such standards and requirements should be scaled proportionally, while taking into consideration factors such as the size of a business and its financial resources. The federal framework should be promulgated and enforced by a specialized federal cybersecurity governance organization.

INTRODUCTION

In 2008, a small web-based business called MyBizHomepage launched a revolutionary new analytics tool to equip other small businesses with better financial management solutions.[1] The resounding success of its new product propelled MyBizHomepage's valuation to $100 million[2] until 2009, when the

1. *MyBizHomepage Launches New Platform to Help Small Businesses*, BUS. WIRE (Aug. 6, 2008, 2:11 PM), https://www.businesswire.com/news/home/20080806006074/en/MyBiz Homepage-Launches-New-Platform-Small-Businesses.

2. Darren Dahl, *Struggling to Recover from a Cyberattack*, N.Y. TIMES (Aug. 22, 2012), https://www.nytimes.com/2012/08/23/business/smallbusiness/struggling-to-recover-from-a-cyberattack.html.

company fell victim to a devastating cyberattack.[3] Cybercriminals[4] infiltrated MyBizHomepage's proprietary software, resulting in the unauthorized release of its founder's personal information, as well as that of his family, friends, and investors.[5] Faced with rapidly depleting financial resources after several failed attempts to remedy the breach, founder Peter Justen contemplated whether to declare corporate bankruptcy or permanently close his business in favor of compensating its vendors,[6] many of whom had immediately filed suit for unpaid bills following the cyberattack.[7] Reluctantly, Justen closed MyBizHomepage at the pinnacle of its popularity. He decided that its closure was preferable to bankruptcy, because bankruptcy would not only force Justen's company out of business but also compromise its intellectual property rights and render it extremely difficult to attract investors for future business endeavors.[8]

---

3. A "cyberattack" or "cyber attack," which are synonyms, the former of which is used throughout this Note, is defined as:

> A hostile act using computer or related networks or systems . . . intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. . . . not necessarily limited to the targeted computer systems or data themselves . . . . A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The . . . effect . . . may be widely separated temporally and geographically from the delivery.

Oona A. Hathaway et al., *The Law of Cyber Attack*, 100 CAL. L. REV. 817, 824 (2012) (quoting Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. Of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (Nov. 2011)).

4. A "cybercriminal" is defined as:

> [A]n individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both. Cybercriminals . . . attack other people's computers to perform malicious activities, such as spreading viruses, data theft, identity theft, etc. . . . use the computer to carry out "conventional crime," such as spam, fraud, illegal gambling . . . . [or] to save stolen or illegal data.

Cybercriminal, TECHOPEDIA, https://www.techopedia.com/definition/27435/cybercriminal (last visited Nov. 24, 2018).

5. Karen E. Klein, *How Business Owners Counter Online Slander*, BLOOMBERG (Oct. 25, 2011, 12:15 PM), https://www.bloomberg.com/news/articles/2011-10-25/how-business-owners-counter-online-slander.

6. Darren Dahl, *Starting Over After a Cyberattack Shuts Down the Business*, N.Y. TIMES (Aug. 29, 2012, 7:00 AM), https://boss.blogs.nytimes.com/2012/08/29/starting-over-after-a-cyberattack-shuts-down-the-business.

7. *Id.*; Klein, *supra* note 5.

8. *See* Dahl, *supra* note 6.

MyBizHomepage is just one of many small businesses to be confronted with this agonizing decision due to a cyberattack.[9] Following a cyberattack in 2014, Code Spaces,[10] an innovative Software as a Service (SaaS)[11] provider, was forced to permanently close its business when cybercriminals commandeered the systems integral to its operations and demanded a hefty ransom to cease the attack.[12] By the time Code Spaces regained control of its systems, most of its crucial operational data files had been permanently deleted.[13] In a since-removed online post that resided on its former business website, Code Spaces cited the resulting financial difficulties and loss of consumer confidence caused by the breach as the catalysts for its closure.[14]

Small businesses are at a greater risk of failure due to cyberattacks because they must navigate a minefield of data security risks while complying with data protection and breach notification laws identical to those of larger businesses.[15] Unlike their larger counterparts, however, small businesses lack the financial resources and technological sophistication to mitigate such data security risks or endure the legal and remedial ramifications of a data breach.[16] Compounding their risk of failure is the current disjointed federal and state statutory data protection and breach notification scheme, which plagues small firms with inconsistent legal requirements and disproportionately large monetary penalties.[17]

---

9. Indeed, many small businesses have suffered the consequence of cyberattacks, especially due to the unwillingness of financial institutions to cover the loss. *See* John Ydstie, *When Cyberfraud Hits Businesses, Banks May Not Offer Protection*, NPR (Sept. 15, 2015, 5:04 AM), https://www.npr.org/sections/alltechconsidered/2015/09/15/440252972/when-cyber-fraud-hits-businesses-banks-may-not-offer-protection; *see also 3 Companies that Went Out of Business Due to a Security Breach*, PRO ON CALL TECH. (Nov. 6, 2014), https://prooncall.com/3-companies-went-business-due-security-breach; Jane Chen, Note, *Cyber Security: Bull's-Eye on Small Businesses*, 16 J. INT'L BUS. & L. 97, 102 (2016).

10. *See* Steve Ragan, *Code Spaces Forced to Close its Doors After Security Incident*, CSO (June 18, 2014, 1:03 PM), https://www.csoonline.com/article/2365062/disaster-recovery/code-spaces-forced-to-close-its-doors-after-security-incident.html; *see also* Chen, *supra* note 9, at 102–03.

11. A SaaS is defined as "a company that hosts an application and makes it available to customers over the internet. . . . This infers that the software sits on a SaaS company's server while the user accesses it remotely." Chris Brook, *What is a SaaS Company?*, DIGITAL GUARDIAN (Dec. 4, 2018), https://digitalguardian.com/blog/what-saas-company; *see also* Chen, *supra* note 9, at 102.

12. *See* Ragan, *supra* note 10.

13. *See id.*

14. *Id.* ("Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in a irreversible position both financially and in terms of on going credibility.").

15. *See* Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?*, 13 J. BUS. & TECH. L. 217, 218 (2018); Luis A. Aguilar, *The Need for Greater Focus on the Cybersecurity Challenges Facing Small Business*, U.S. SEC. & EXCH. COMM'N (Oct. 22, 2015), https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html.

16. *See* Selznick & LaMacchia, *supra* note 15, at 218; Aguilar, *supra* note 15; *see also* Chen, *supra* note 9, at 100.

17. *See* Chen, *supra* note 9, at 107–08; Selznick & LaMacchia, *supra* note 15, at 240–42.

This Note argues that, in the interest of preserving the viability of small businesses in the event of a cyberattack, Congress must temporarily streamline the current state-based statutory scheme and industry-targeted federal approach to data protection and breach notification laws. Then, Congress must enact a comprehensive data protection and breach notification framework in a centralized, multi-tiered federal program. The applicability of the program's provisions to a business should be scaled in accordance with the business' size, financial resources, and implementation of minimum cybersecurity standards.[18] Lastly, the new framework must be closely managed and enforced by a federally created, centralized cybersecurity governance organization.

Part I of this Note explains the integral role of small businesses in bolstering a healthy U.S. economy. Part II introduces the history of data breaches and the resulting patchwork of state-based and industry-specific federal data protection and breach notification laws. Part III analyzes the impact of the current data protection and breach notification legal framework on the viability of small businesses. Part IV explores the potential impact of recently enacted data privacy laws on the viability of small businesses. Part V discusses the need to federalize data protection and breach notification laws. Finally, Part VI proposes a plan for Congress to implement a federal solution that will benefit businesses of all sizes and equip small businesses to comply with consistent data protection and breach notification laws by using the financial and technological resources small businesses already have available.

I. SMALL BUSINESSES BUILD THE AMERICAN ECONOMY

The term "small business"[19] commonly evokes a quaint picture of a locally-owned mom and pop shop.[20] In reality, small businesses transcend

18. "Cybersecurity" has different contextual applications, but in the context of data protection (and in this Note), it refers to "information security measures that custodians of consumer data take to protect such sensitive information." David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 292 (2014) (footnotes omitted).

19. ROBERT JAY DILGER, CONG. RESEARCH SERV., SMALL BUSINESS SIZE STANDARDS: A HISTORICAL ANALYSIS OF CONTEMPORARY ISSUES (2019), https://fas.org/sgp/crs/misc/R40860.pdf (stating that the U.S. Small Business Administration's definition of a "small business" considers "size standards [that] are based on one of four measures: (1) number of employees, (2) average annual receipts, (3) average asset size as reported in the firm's four quarterly financial statements for the preceding year, or (4) a combination of number of employees and barrel per day refining capacity"); *see Size Standards*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/federal-contracting/contracting-guide/size-standards (last visited Nov. 25, 2018); U.S. SMALL BUS. ADMIN., TABLE OF SMALL BUSINESS SIZE STANDARDS (2017), https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2017.pdf.

20. *See* Major L. Clark, III & Radwan N. Saade, *The Role of Small Business in Economic Development of the United States: From the End of the Korean War (1953) to the Present*, U.S. SMALL BUS. ADMIN. (Sept. 1, 2010), https://www.sba.gov/advocacy/role-small-business-economic-development-united-states-end-korean-war-1953-present; Mike Moffatt, *Small Business*

their limited role as mere romanticized imagery of the American Dream;[21] they are the foundation on which the robust U.S. economy stands.[22] As of August 2018, there were 30.2 million small businesses in the United States comprising 99.9% of all American businesses and accounting for nearly 48% of private sector employment in the United States.[23] Without small businesses, the United States stands to lose almost half of its workforce and most of its independent businesses.[24]

Small businesses are the driving force of American economic growth. Approximately seven out of every ten new jobs are created by small businesses.[25] Additionally, of "high patenting" businesses,[26] small businesses spearhead American innovation and earn an impressive per-employee rate of sixteen times more patents on average than their larger corporate counterparts.[27] Further, the private sector manages more than 90% of the country's critical infrastructure, including its sensitive data.[28] The stability of America's employment rate, innovative leadership, and safety of its critical infrastructure depend largely on the health of its small business economy.[29]

Recognizing the impact of small business on the welfare of the American economy, Congress has historically intervened at times when the viability of

---

in the United States, THOUGHTCO. (July 3, 2019), https://www.thoughtco.com/intro-to-small-business-in-the-united-states-1147915.

21. "The American Dream" is a term used to capture the set of ideals of life in the United States. *See American Dream*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/the%20American%20dream (last visited Nov. 25, 2018).

22. *See The Importance of Small Business to the U.S. Economy*, U. MINN. LIBR., http://open.lib.umn.edu/exploringbusiness/chapter/5-2-the-importance-of-small-business-to-the-u-s-economy (last visited Nov. 25, 2018) [hereinafter *Importance of Small Business*]; *see also* Chen, *supra* note 9, at 118.

23. *See* U.S. SMALL BUS. ADMIN., 2018 SMALL BUSINESS PROFILE 1 (n.d.), https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf; *see also* U.S. SMALL BUS. ADMIN., WHAT'S NEW WITH SMALL BUSINESS? (2018), https://www.sba.gov/sites/default/files/Whats-New-With-Small-Business-2018.pdf.

24. *See* WHAT'S NEW WITH SMALL BUSINESS?, *supra* note 23; *see also* Amanda Cameron, *What is Considered A Small Business?*, PATRIOT SMALL BUS. (July 14, 2017), https://smallbusiness.patriotsoftware.com/what-is-considered-small-business-classification-size (defining an "independently owned" small business for purposes of the U.S. Small Business Administration as one that is "not owned by a parent corporation").

25. Steve Chabot, *Why Small Business Is the Key to Our Economy*, INC. (Mar. 4, 2015), https://www.inc.com/steve-chabot/building-an-opportunity-economy-starts-with-small-business.html; *see also* Moffat, *supra* note 20.

26. Robert Longley, *How Small Business Drives U.S. Economy*, THOUGHTCO. (Mar. 2, 2018), https://www.thoughtco.com/how-small-business-drives-economy-3321945 (explaining that a "high patenting" business is one that is granted fifteen or more patents per four years).

27. *Id.*

28. *See* Scott J. Shackelford et al., *How Businesses Can Support Cyber Peace*, 36 U. PA. J. INT'L L. 353, 359 (2014); *see also* Brian Harrell, *The Private Sector Is the Key to Success for the Department of Homeland Security*, CSO (Feb. 1, 2017, 5:47 AM), https://www.csoonline.com/article/3161793/security/the-private-sector-is-the-key-to-success-for-the-department-of-homeland-security.html.

29. *See generally* 2018 SMALL BUSINESS PROFILE, *supra* note 23 (displaying small business statistics and their economic impact).

small businesses has been at risk.[30] For example, during the economic downturn caused by the Great Depression and World War II, masses of well-established small businesses faltered to procure business, and many failed.[31] In response to the crisis, Congress, via the Small Business Act of 1953, created the U.S. Small Business Administration (SBA), an advocacy and governance organization in support of small businesses.[32] In describing the purpose of the Small Business Act, Congress affirmed the importance of small business survival to the economy by writing into the law, in part:

> The essence of the American economic system of private enterprise is free competition. . . . The preservation and expansion of such competition is basic not only to the economic well-being but to the security of this Nation. Such security and well-being cannot be realized unless the actual and potential capacity of small business is encouraged and developed. It is the declared policy of the Congress that the Government should aid, counsel, assist, and protect, insofar as is possible, the interests of small-business concerns . . . to maintain and strengthen the overall economy of the Nation.[33]

Congressional action in response to threats to the viability of small businesses is paramount to their survival.[34] Congress created the SBA to ensure the survival and further the interests of small businesses, which bolstered America's overall postwar economic repair and growth.[35] Since its inception, the SBA has aided in the success of small businesses through

30. *See* 15 U.S.C. § 631(a) (2012) ("It is the declared policy of the Congress that the Government should aid, counsel, assist, and protect, insofar as is possible, the interests of small-business concerns . . . .").

31. *See Revival of Small Business*, CQ RESEARCHER, https://library.cqpress.com/cqresearcher/document.php?id=cqresrre1945032100#H2_3 (last visited Nov. 25, 2018)

> Wartime requirements for rapid production and quick action on war contracts have accentuated a prewar trend toward concentration . . . . At the same time many small concerns engaged in service and distribution activities, and in production of luxury goods, have found it necessary to curtail or cease operations for lack of manpower and materials. . . . Fears have been widely expressed that wartime changes and wholesale business terminations have sounded the death knell of small business enterprise in the United States.

Id.

32. *See About SBA: Organization*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/about-sba/organization (last visited Dec. 26, 2019); *Small Business Act: Policy Guidance*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/document/policy-guidance--small-business-act (last visited Dec. 26, 2019); *Small Business Administration*, OFF. FED. REG., https://www.federalregister.gov/agencies/small-business-administration (last visited Nov. 25, 2018); *see also* S. REP. NO. 81-1263, at 10 (1950).

33. 15 U.S.C. § 631(a); *see also* ROBERT JAY DILGER, CONG. RESEARCH SERV., SBA'S "8(A) PROGRAM": OVERVIEW, HISTORY, AND CURRENT ISSUES 3 (2019), https://fas.org/sgp/crs/misc/R44844.pdf.

34. *See, e.g.*, *About SBA: SBA Initiatives*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/about-sba/organization/sba-initiatives (last visited Dec. 26, 2019).

35. *See* Mirit Eyal-Cohen, *Why Is Small Business the Chief Business of Congress?*, 43 RUTGERS L.J. 1, 4 (2012); *About SBA: Organization*, *supra* note 32.

initiatives providing access to capital, entrepreneurial education, incentivization for government contracting, and general advocacy.[36] As it did during the economic downturn following World War II, Congress must assess the economic risks of the current cybersecurity landscape on small businesses and again advocate for such businesses to ensure their longevity.

II. THE RAPID GROWTH OF DATA SECURITY RISKS AND CURRENT DATA PROTECTION AND BREACH NOTIFICATION LAWS

Cybersecurity challenges on the rise since the late 1980s have necessitated the creation of laws that govern the protection of consumer data collected by businesses.[37] However, small businesses have struggled to stay afloat in the wake of rapidly growing data security risks[38] and the resulting implementation of disjointed state-based and industry-specific data protection and breach notification laws. In 2017 alone, cybercriminals targeted 60% of the 29.6 million small businesses in the United States.[39] Every year, of the small businesses whose data is compromised, a staggering 60% fail within a mere six months due to the loss of consumer trust, the financial burden of remedying the breach, paying penalties, and reimbursing investors, consumers, and other affected parties.[40] News media outlets tend to publicize high-profile breaches at larger companies due to the substantial quantity of records involved.[41] However, it is smaller firms that are more frequently targeted by cybercriminals and at the greatest risk of failing following a cyberattack.[42]

---

36. *See About SBA: Organization*, *supra* note 32; *About SBA: SBA Initiatives*, *supra* note 34.

37. *See generally Cybersecurity, A Timeline*, UPPER MIDWEST SECURITY ALLIANCE (Feb. 28, 2017), https://umsa-security.org/cybersecurity-a-timeline; *Data Breaches*, PRIV. RTS. CLEARINGHOUSE, https://privacyrights.org/data-breaches?title=&taxonomy_vocabulary_11_tid%5B%5D=271 (last visited Dec. 26, 2019) (providing a download link for a spreadsheet containing data breach information from January 2005 through October 2019).

38. *See* Thomas Koulopoulos, *60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)*, INC.: INNOVATE (May 11, 2017), https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html.

39. *See 5 Cybersecurity Statistics Every Small Business Should Know in 2018*, ALERT LOGIC (May 14, 2018), https://blog.alertlogic.com/5-cybersecurity-statistics-every-small-business-should-know-in-2018 [hereinafter *5 Cybersecurity Statistics*]; Elizabeth Leary, *Local Businesses a Target for Next Cyberattacks*, CNBC (Oct. 13, 2017, 8:53 AM), https://www.cnbc.com/2017/10/13/local-businesses-a-target-for-next-cyberattacks.html; 2018 SMALL BUSINESS PROFILE, *supra* note 23.

40. *See* Chen, *supra* note 9, at 100; Koulopoulos, *supra* note 38.

41. For example, a large, highly publicized data breach occurred at Target stores in 2012, which resulted in the exposed credit card and personal information of over 110 million of its consumers. *See E-mail Attack on Vendor Set Up Breach at Target*, KREBS ON SECURITY (Feb. 14, 2014), https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target [hereinafter *Breach at Target*]; *see* Aguilar, *supra* note 15; *see also In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1307 (D. Minn. 2014); Selznick & LaMacchia, *supra* note 15, at 218.

42. *See* Aguilar, *supra* note 15.

A. STATE LAWS

Current data breach notification laws are primarily matters of state legislation.[43] In 2003, California enacted Civil Code Sections 1798.29 and 1798.82[44] in response to the troubling increase in identification theft. The new law required that all agencies and businesses in possession of personal information facilitate the prompt disclosure of data breaches or suspected data breaches.[45] In 2005, the Privacy Rights Clearinghouse recorded 136 data breaches,[46] which have since increased exponentially each year.[47] The ChoicePoint data breach in 2005 was one of the first to be highly-publicized, and as such, validated California's new law. ChoicePoint, a business that sells personal information, discovered that it had inadvertently sold 145,000 records containing such information to a criminal organization.[48] ChoicePoint immediately notified California residents as to the unauthorized disclosure of their personal information.[49] This swift notification protocol prevented the potential for additional damages and costs to accrue had California's law not been enacted.

In the haste to create laws requiring the disclosure of data breaches following ChoicePoint and several other high-profile breaches, each state followed California's lead.[50] By March 2018, all fifty states had enacted data breach notification laws.[51] As a consequence, businesses of all sizes, locations, and revenue levels are required to comply with breach notification rules that vastly differ by state.

B. FEDERAL LAWS

Several federal administrative agencies have also enacted regulatory guidelines and data protection laws covering a limited scope of industry-

43. *See Breach Notification Law Interactive Map*, BAKER & HOSTETLER LLP, https://www.bakerlaw.com/BreachNotificationLawMap (last visited Nov. 25, 2018) [hereinafter *Interactive Map*].

44. CAL. CIV. CODE §§ 1798.29, 1798.82 (Deering, LEXIS through 2020 Sess.).

45. *See* CIV. CODE §§ 1798.29, 1798.82; Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals with ID Theft: The Promise and the Problems*, 13 AM. BAR ASS'N: ABA BUS. L. SEC. (May 2004), https://www.americanbar.org/content/dam/aba/publications/blt/2004/05/calinfornia-deals-with-id-theft-200405.authcheckdam.pdf.

46. *Data Breaches*, *supra* note 37.

47. *See* Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN DATA INSIDER (Apr. 6, 2018), https://digitalguardian.com/blog/history-data-breaches.

48. *See* Samuel Lee, Note, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L.J. 125, 127–28 (2006).

49. *See Breach of Information*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/overview-security-breaches.aspx (last visited Sept. 28, 2018).

50. *See id.*

51. *See* Julie Hein, *Navigating the State Data Breach Laws? An Enhanced Resource Is Available*, DATA PRIVACY MONITOR (Sept. 21, 2018), https://www.dataprivacymonitor.com/data-breach-notification-laws/navigating-the-state-data-breach-laws-an-enhanced-resource-is-available.

specific entities and data types. Three types of data specifically addressed by federally enacted laws are: (1) Personally Identifiable Information (PII),[52] (2) consumer credit reporting information, and (3) Protected Health Information (PHI).[53]

Theoretically, federal data protection and breach notification laws should positively impact the preservation of small businesses. These laws often create *de facto* data security standards that preempt and transcend the scope of state-enacted statutes by offering businesses across the United States a consistent framework under which to structure their data protection policies.[54] Nevertheless, the practical application of current federal data protection and breach notification regulations to small business is rare because these regulations impact only a narrow scope of data types[55] and business institutions.[56]

1. The Gramm-Leach-Bliley Act

In 1999, Congress enacted the Gramm-Leach-Bliley Act (GLBA),[57] which places the burden on financial institutions to affirmatively ensure adequate protection against unauthorized use of their consumers' PII via mandated minimum data security standards.[58] In practice, this law's applicability is narrow, as it only pertains to a specific type of data—PII—held by a limited scope of businesses—financial institutions.[59] The GLBA defines "financial institutions" identically to the Bank Holding Company Act of 1956,[60] which describes such institutions as those "engaging in activities that are financial in nature."[61] Due to the GLBA's vague definition of "financial institutions," its applicability to certain types of businesses is unclear. However, courts have consistently decided GLBA cases involving

52. *See* Chen, *supra* note 9, at 105.

53. *See* Thaw, *supra* note 18, at 327.

54. *See id.* at 293.

55. Often, only one of PII, PHI, or consumer credit reporting information.

56. *See, e.g.*, Selznick & LaMacchia, *supra* note 15, at 245 ("The FTC has suggested that, for economic reasons, it expects less data security from small businesses.").

57. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09, 6821–27 (2012).

58. *See* Edward J. Janger & Paul M. Schwartz, *Modern Studies in Privacy Law: Notice, Autonomy, and Enforcement of Data Privacy Legislation: The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1229–30 (2002) ("The GLB Act spells out three requirements for data security. It calls for financial institutions to (1) protect the security and confidentiality of customer records and information; (2) prevent any anticipated threats or hazards to the security or integrity of such records; and (3) prevent unauthorized access to use of records that could result in "substantial harm or inconvenience to any customer."); Lee, *supra* note 48, at 127.

59. *See* 12 U.S.C. § 1843(k) (2018).

60. *See id.*

61. *See id.*

primarily large banking and insurance institutions, resulting in the rare judicial applicability of this law to small businesses.[62]

2. The Health Insurance Portability and Accountability Act of 1996

Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[63] to restrict the unauthorized disclosure of consumer personal health information.[64] Similar to the GLBA, HIPAA offers consistent rules as to data protection and breach notification, but it applies narrowly to businesses in possession of PHI and is limited to "health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically."[65] Thus, HIPAA does not apply to small businesses, except in instances where small businesses are also small health care providers, such as private medical practices.[66] However, health care and insurance-based businesses comprise only a combined 13% of all small businesses.[67] Consequently, HIPAA's practical applicability to small businesses remains low.

3. The Federal Trade Commission

In 1914, Congress created the Federal Trade Commission (FTC) in an effort to protect consumers from unfair trade practices.[68] In its role of protecting consumers, the FTC has evolved, in part, to be a "gap-filler" for other federal laws regulating data protection and breach notification

62. *See, e.g.*, Am. Bar Ass'n v. Fed. Trade Comm'n, 430 F.3d 457, 470 (D.C. Cir. 2005) (denying FTC enforcement of attorneys under the GLBA because "attorneys and law firms, even if viewed as 'institutions,' are not institutions 'the business of which is engaging in financial activities,' as defined in the statute"); Quadrant Info. Servs., LLC v. LexisNexis Risk Sols., Inc., No. C 11-6648 SBA, 2012 U.S. Dist. LEXIS 108597, at *11–12 (N.D. Cal. July 31, 2012) (holding that "[Plaintiff] has failed to allege a cognizable claim under the GLBA . . . [because Plaintiff] does not allege in its Complaint or claim in its opposition brief that LexisNexis is a 'financial institution.' On that basis alone, the GLBA is inapplicable to LexisNexis").

63. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; *see Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

64. *See* Chen, *supra* note 9, at 110.

65. *See HIPAA for Professionals*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/index.html.

66. *See* Selznick & LaMacchia, *supra* note 15, at 222–25; *HIPAA for Professionals*, *supra* note 65.

67. *See What Industries Are Small Businesses In?*, U. MINN. LIBR., https://open.lib.umn.edu/exploringbusiness/chapter/5-3-what-industries-are-small-businesses-in (last visited Oct. 28, 2018).

68. *See About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Dec. 26, 2018).

protocols.[69] The FTC pursues data security-related administrative actions against businesses engaged in "unfair or deceptive acts or practices" in violation of Section 5 of the FTC Act.[70] These actions are often brought in conjunction with other federal statutes, such as the Fair Credit Reporting Act.[71] Although the FTC does not formally restrict its actions to businesses based on size, like its federal regulatory companions, most actions are brought against larger companies that disclose, sell, or allow unauthorized access to various data types, including consumer credit reporting information. In practice, the FTC does not often bring actions against small businesses.[72]

The current legislative framework imposes inconsistent data protection and breach notification guidelines on small businesses. State-enacted statutes vary substantively by state, while equally deficient industry-specific federal laws only govern certain data types with applicability to a limited scope of businesses. The result is confusion and increased data breach vulnerability, as small businesses are forced to comply with numerous enigmatic rules.

III. CURRENT DATA PROTECTION AND BREACH NOTIFICATION LAWS ARE A THREAT TO THE LONGEVITY OF SMALL BUSINESS

With rapid advances in technology further emboldening cybercriminals, an exponentially increasing threat of cyberattacks looms over small businesses.[73] Current state-based data protection and breach notification laws only contribute to the vulnerability of small businesses because such laws: (A) are inconsistently applied and impose disproportionately high penalties, (B) contain varying definitions of identical terminology and different applicability criteria by state, (C) vary in judicial interpretation by state, (D) impose different jurisdictional requirements by state, and (E) place targets on small businesses because of their access to data from working with larger businesses. Additionally, Congress has failed to enact comprehensive federal data protection laws geared toward all types of businesses and data. As a result, small businesses grapple with unnecessary regulatory confusion and roadblocks to compliance.[74]

69. *See* Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement under Section 5*, AM. BAR ASS'N, http://web.archive.org/web/20170202135520/http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html.html (last visited Feb. 18, 2020).

70. *See* 15 U.S.C. § 45(a)(1) (2012); Woods, *supra* note 69.

71. Woods, *supra* note 69.

72. *See* Selznick & LaMacchia, *supra* note 15, at 245.

73. *See 5 Cybersecurity Statistics*, *supra* note 39.

74. *See* Selznick & LaMacchia, *supra* note 15, at 226–27.

A. INCONSISTENT APPLICATION AND DISPROPORTIONATE PENALTIES OF STATE-BASED LAWS

State-enacted data protection and breach notification statutes often do not restrict application to a business based on its size, location, or income. Instead, in an effort to protect intrastate consumers, these laws apply to all businesses within the United States and are broadly based on whether a business' affected consumers are residents located *in that state*.[75] By way of example, California's data breach notification law[76] requires that any business possessing the personal information of California residents comply with the breach notification rules in California with respect to those resident consumers.[77] Thus, if a small business in New Mexico discovers or suspects a data breach, it must first identify its affected consumers who reside in California, then notify them of the data breach in accordance with the requirements under California's data breach notification law.[78] Next, the small business in New Mexico would need to expend additional resources investigating the breach notification requirements for its affected consumers located in each of the other forty-nine states. Ultimately, the business may incur crippling costs to remediate the breach that, across the United States, averages $233 per record breached.[79] In 2011, non-employer small businesses earned an average yearly revenue of $44,000.[80] A small business with this annual revenue could potentially lose all of its income for the year if a mere 189 records are breached, which is well within the realm of possibility for a small business. Further impacting the overall cost is that some states have significantly larger per-record monetary penalties than others, which in the aggregate could far exceed a small business' revenue.[81]

Following a data breach, the civil monetary penalties imposed on a small business by just one state may threaten its viability, let alone the civil penalties of other states where a small business is also likely to have affected customers. In *Commonwealth v. Haney*, the Commonwealth of Massachusetts commenced a consumer protection action against defendant Haney, a solo practicing real estate attorney, for failing to protect his clients' personal information when he neglected to securely dispose of their personal

75. *See* Paetkau & Torabian-Bashardoust, *supra* note 45; Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, LAW TECH. TODAY (Apr. 19, 2016), https://www.lawtechnologytoday.org/2016/04/crazy-quilt-work-state-data-breach-notification-laws-just-got-crazier.

76. CAL. CIV. CODE § 1798.82 (Deering, LEXIS through 2020 Sess.); *see* Paetkau & Torabian-Bashardoust, *supra* note 45.

77. *See* Paetkau & Torabian-Bashardoust, *supra* note 45.

78. *Id.*

79. *See* PONEMON INST. LLC, 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 13 (2018), https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

80. *See* Jason Nazar, *16 Surprising Statistics About Small Business*, FORBES (Sept. 9, 2013, 10:20 AM), https://www.forbes.com/sites/jasonnazar/2013/09/09/16-surprising-statistics-about-small-businesses/#2e1c0a215ec8.

81. *See Interactive Map*, *supra* note 43.

records.[82] The Superior Court of Massachusetts held that Haney's actions violated the Massachusetts Security Breaches Law,[83] which requires compliance with regulations "designed to safeguard the personal information of residents of the commonwealth," and that such regulations apply to "any person that owns or licenses personal information about a resident of the commonwealth."[84] Pursuant to the law, the Superior Court entered judgment against Haney for civil penalties in the amount of $10,000.[85]

While a large corporate entity may not balk at a monetary penalty of $10,000, a small business may not be able to survive such a fine. The Massachusetts law applied in *Haney* concerns businesses of all sizes and protects only "the personal information of residents of the commonwealth."[86] Thus, Haney may be exposed to additional lawsuits and monetary penalties leveraged by other states' data protection and breach notification laws,[87] because the civil penalty of $10,000 imposed on Haney only reflects the penalties for his clients who are residents of Massachusetts in violation of Massachusetts law.[88]

As discussed above, the average non-employer small business makes $44,000 per year.[89] In 2017, solo practicing attorneys earned an average of $148,000 nationally.[90] Assuming Haney is an average solo practitioner who earns an annual salary of approximately 3.36 times more than the average non-employer small business, even a $10,000 penalty for the breach of personal information of his clients located in *just one state* makes up about 7% of his business' yearly income. Such a financial hit could be fatal to a solo practicing attorney, let alone the average small business, even if that small business does not have clients in other states and no additional lawsuits are brought. Indeed, if other states brought actions against Haney on behalf of his clients residing in those states, he could be responsible for paying more in civil penalties than he makes in one year.

82. *See* Commonwealth v. Haney, No. 16-00183, 2016 Mass. Super. LEXIS 915, at *2–4 (Mass. Dist. Ct. Jan. 12, 2016).

83. *See* MASS. ANN. LAWS ch. 93H (LEXIS through 2020 Legis. Sess.).

84. *See id.* § 2(a).

85. *See Haney*, 2016 Mass. Super. LEXIS 915, at *9.

86. *See* ch. 93H, § 2(a).

87. *See* Embry, *supra* note 75.

88. *See Haney*, 2016 Mass. Super. LEXIS 915, at *7–9.

89. Nazar, *supra* note 80.

90. MARTINDALE-AVVO, 2019 ATTORNEY COMPENSATION REPORT 8 (2019), https://www.martindale-avvo.com/wp-content/uploads/2019-Attorney-Compensation-Report.pdf.

B. STATE-BASED LAWS CONTAIN VARYING DEFINITIONS FOR IDENTICAL TERMS AND DIFFERENT CRITERIA FOR APPLICABILITY

Another issue is the lack of standardized definitions of identical terms among state laws.[91] While the term "personal information" is used routinely in each state's breach notification law, the definition of "personal information" varies drastically from state to state.[92] For example, in California, "personal information" is defined as:

> (1) An individual's first name or first initial and last name *in combination with* any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number[,] (B) Driver's license number . . . or other unique identification number issued on a government document[,] . . . (C) Account number or credit card number in combination with any required security code . . . that would permit access to an individual's financial account[,] (E) Medical information[,] (F) Health insurance information[,] (F) Unique biometric data[,] . . . (G) Information or data collected through the use or operation of an automated license plate identification system[,] . . . [or] (2) A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.[93]

In Indiana, "personal information" is more narrowly defined in part as:

> (1) a social security number, . . . or . . . (2) an individual's first and last names, and one . . . or more of . . . (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 . . . that would permit access to the person's account.[94]

Indiana's definition of "personal information" does not include certain combinations of information considered "personal information" in California. Adding to the confusion is that Indiana's and California's provisions overlap in other ways. For example, both states limit the meaning of a breach of personal information to unencrypted data, or encrypted data where the encryption key is also compromised.[95]

---

91. *See* Lee, *supra* note 48, at 130–31; *Interactive Map*, *supra* note 43.

92. *Interactive Map*, *supra* note 43.

93. CAL. CIV. CODE § 1798.82(h) (Deering, LEXIS through 2020 Sess.) (emphasis added); *see* Lee, *supra* note 48, at 132.

94. IND. CODE ANN. § 24-4.9-2-10 (Burns, LEXIS through P.L. 153-2020 of 2020 2nd Reg. Sess. of 121st General Assemb.).

95. *Compare* CAL. CIV. CODE § 1798.82(a) (Deering, LEXIS through 2020 Sess.), *with* IND. CODE ANN. § 24-4.9-2-2(b)(2) (Burns, LEXIS through P.L. 153-2020 of 2nd Reg. Sess. of 121st General Assemb.).

Additionally, state-enacted data protection and breach notification laws define different circumstances by which their applicability is triggered. For example, Arkansas' data breach notification law outlines a significant exemption that California's does not. In Arkansas, notification requirements do not apply when a "business determines that there is no reasonable likelihood of harm to customers."[96] This provision allows a business to elect not to notify its affected consumers of a data breach if it concludes that there is no reasonable likelihood that harm to its customers will result.[97] In addition to small businesses' general lack of sophisticated technological and financial resources, state-based laws that contain varying criteria for applicability impede small businesses from implementing effective cybersecurity strategies to ensure legal compliance.

C. DIFFERENCES IN THE JUDICIAL INTERPRETATION OF STATE-BASED LAWS

Even when the language of a state-enacted statute is clear on its face, the court hearing a lawsuit may interpret the law in unexpected ways, making its application difficult for small businesses to anticipate. For example, in *In re Yahoo! Inc. Customer Data Security Breach Litigation*,[98] the Northern District of California rejected defendant Yahoo!'s argument that it was not in breach of California's Customer Records Act.[99] Yahoo! contended that because California's law defined "personal information" in relevant part as "an individual's user name or email address, in combination with a password or security question and answer that would permit access to an online account,"[100] it could not be in breach since the cybercriminals who accessed Yahoo!'s users' e-mail accounts did so *without* obtaining their passwords.[101] In holding that the information stolen still constituted "personal information," the court reasoned that:

96. ARK. CODE ANN. § 4-110-105(d) (LEXIS through 2020 1st Extraordinary Sess.); *see also* Lee, *supra* note 48, at 133–34.

97. *See* Lee, *supra* note 48, at 134.

98. *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212 (N.D. Cal. Aug. 30, 2017).

99. *See* CAL. CIV. CODE § 1798.82 (Deering, LEXIS through 2020 Sess.).

100. *See In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212, at *139 (N.D. Cal. Aug. 30, 2017) (internal quotation marks omitted) (quoting CIV. § 1798.82(h)).

101. *See id.* at *139–43.

> [E]ven if the . . . [b]reach did not involve hackers gaining access to users' [e-mail] passwords, Plaintiffs allege that the . . . [b]reach nonetheless involved hackers gaining access to other types of information that [Cal. Civ. Code] § 1798.82(h) defines as "personal information," such as "social security number[s]," "medical information," or "credit or debit card number[s]."[102]

In sum, even though California's law clearly states that "personal information" in the context of *In re Yahoo! Inc.* consists of a user name in combination with a password, the court held the specificity of the law's language was irrelevant because the cybercriminals gained access to the systems *as if* they had obtained the passwords providing them with unauthorized access to Yahoo!'s users' additional personal information.[103] While Yahoo! is a large business with the financial resources to manage the monetary burden of such a decision, a small business may not be able to shoulder the financial blow, which could occur even if it made a good faith effort to comply with a state law's exact language. The burden on small businesses is unfairly imposed. In order to adequately safeguard against and contend with a breach, small businesses must not only consider how each state defines its law's terms but also the ways in which each state's courts may interpret the meaning of such terms.

D. JURISDICTIONAL REQUIREMENTS VARY IN STATE-BASED LAWS

Some states require that breach notification enforcement actions be handled by the Attorney General (AG) of that state, while other states allow a private right of action to sue.[104] The result of this difference in practice is that a court may expend already scarce personnel resources, and parties may sustain effort and unnecessary costs litigating a case to later discover the claim can only be brought by that state's AG. Likewise, a complaint may be lodged with a state's AG when, after time and money is spent pursuing that complaint, the AG informs the complainant that he or she must bring the action before a state court.

In *Community Bank of Trenton v. Schnuck Markets*, defendant Schnuck fell victim to a data breach that compromised the data of approximately 2.4 million credit cards from its seventy-nine stores.[105] Plaintiff Trenton alleged that Schnuck failed to timely report the breach to its consumers in violation of Missouri's breach notification law.[106] Trenton claimed Schnuck had discovered the breach on March 19, 2013 and did not report the breach to

102. *See id.* at *143.
103. *See id.* at *144.
104. *See Interactive Map*, *supra* note 43.
105. *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *5–6 (S.D. Ill. May 1, 2017).
106. MO. REV. STAT. § 407.1500.2 (LEXIS through 100th General Assemb., 2019 legislation and the 1st extra Sess.).

consumers until eleven days later, which allowed for an additional 340,000 credit card numbers to be compromised.[107] Although the court recognized the allegations as potentially valid,[108] it granted Schnuck's motion to dismiss, stating that "Missouri's . . . data breach notification statute exclusively bestows the power to prosecute violations upon the Missouri Attorney General" and that it "will not read additional [judicial] duties into a law carefully crafted by the legislature."[109] The court further explained that an argument brought by Trenton based upon the decision in *In re Target Corp. Customer Data Security Breach Litigation*, wherein the Minnesota court punished Target for failing to encrypt its customers' data, had no applicability in this case because "the *Target* court relied . . . upon data security provisions unique to Minnesota law—provisions which have no analogue in Missouri law."[110]

E. STATE-BASED LAWS IMPOSED ON SMALL BUSINESSES ARE RISKY TO LARGE BUSINESSES

Large businesses have the financial resources and legal prowess to comply with each of the fifty states' laws, but they too can risk data breach exposure because of the unjust application of those laws to small businesses. Data breach often occurs through small businesses that provide large businesses with materials, supplies, and labor. Such small businesses often have an electronic connection to the large companies for which they perform work. Cybercriminals then exploit these electronic connections to infiltrate the large businesses' systems.[111] Given the breadth of small business relationships to large businesses, the exposure of data breach to large businesses is massive:

> Small firms complement large firms in a number of ways. They supply many of the components needed by big companies. For example, the U.S. automakers depend on more than 1,700 suppliers to provide them with the parts needed to make their cars. . . . [T]here are hundreds of smaller companies that provide a substantial portion of the 8,000 to 12,000 parts that go into each vehicle.[112]

In November 2013, hackers installed malware in Target's computer system to steal the personal consumer payment information of approximately

107. *See Cmty. Bank of Trenton*, 2017 U.S. Dist. LEXIS 66014, at *6.

108. *See id.* at *2.

109. *Id.* at *7; *see also* McNeil v. Best Buy Co., No. 4:13CV1742 JCH, 2014 U.S. Dist. LEXIS 45237, at *12 (E.D. Mo. Apr. 2, 2014) (citing MO. REV. STAT. § 407.1500.4 ("The attorney general shall have exclusive authority to bring an action to obtain actual damages for . . . violation of this section . . . .")).

110. *Cmty. Bank of Trenton*, 2017 U.S. Dist. LEXIS 66014, at *9–10.

111. *See, e.g.*, *Breach at Target*, *supra* note 41.

112. *See Importance of Small Business*, *supra* note 22.

70 million people during the busy holiday shopping season.[113] Earlier in 2013, Target had spent over $1.6 million taking cybersecurity precautions.[114] It was later discovered that the hackers were able to obtain and leverage the vendor login information of Fazio Mechanical Services, a small HVAC business working for Target, to access Target's payment system.[115] Pursuant to Minnesota law, Target paid a $10 million class settlement in connection with the data breach.[116] When all was said and done, Target's breach cost the company an aggregate $162 million in penalties, settlements, and remediation of the breach.[117] Fazio Mechanical Services still appears to be operating, but one of the largest data breaches in history is now associated with its business, which likely has a lasting negative impact on its reputation.

A standardized approach to data protection prevents the likelihood of a damaging data breach to a large business through its relationship with a small business, because businesses of all sizes can comply with a clear set of data security standards. This, in turn, frees up overburdened judicial resources and ensures that the law is justly applied to all entities.

Additionally, current state-based statutes typically address breach notification requirements, but those statutes should do more by establishing minimum security requirements to prevent breach.[118] One of the greatest risks to a small business experiencing a breach is the loss of the business due to the financial ramifications of a breach. Preventative measures, if consistent, accessible, and understood, could be less costly over time. Congress must take action to create a clear, comprehensive cybersecurity framework with small business compliance in mind.

F. CONGRESS HAS FAILED TO ENACT EFFECTIVE FEDERAL DATA LAWS

Congress has failed at several attempts to pass more comprehensive federal regulations with regard to data protection and breach notification.[119] Beginning in 2005, Vermont Senator Patrick Leahy introduced the Personal Data Privacy and Security Act to the 111th Congress, a bill intended "[t]o

113. *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014); *see* Maggie McGrath, *Target Data Breach Spilled Info on as Many as 70 Million Customers*, FORBES (Jan. 10, 2014, 8:56 AM), http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#58dlf7fa6bdl; Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 17, 2014, 10:31 AM), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

114. *See* Riley et al., *supra* note 113.

115. *See Breach at Target*, *supra* note 41.

116. *See* Chen, *supra* note 9, at 107.

117. *See* Natalie Gagliordi, *Target Q4 Boosted by Online, Digital Channels, Data Breach Tallied $162 Million*, ZDNET (Feb. 25, 2015), https://www.zdnet.com/article/target-q4.

118. *See, e.g.*, Lord, *supra* note 47 (providing examples of data breaches due to cybersecurity vulnerabilities).

119. *See* Lee, *supra* note 48, at 136.

prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information."[120] The proposed bill endeavored to federalize state-based breach notifications laws by imposing a consistent, sixty day notification timeline and federal penalties for noncompliance.[121] Unlike state laws, however, the bill would have further obligated businesses in possession of PII to implement a minimum standard of data security measures.[122] Unfortunately, while Senator Leahy brought the bill to Congress each year until 2014, differences in the House of Representatives and the Senate resulted in disagreements that ensured it was never enacted into law.[123]

One of the most comprehensive cybersecurity laws proposals introduced to Congress was the Cybersecurity Act of 2012, which promoted the concepts of penalty-free sharing of cybersecurity threats between the private sector and the federal government, protection of crucial public infrastructure such as water and electricity in case of cyberattack, and authority granted to the Department of Homeland Security (DHS) to manage federal cybersecurity efforts.[124] The bill was promising, but it was ultimately rejected for partisan concerns that it granted excessive power to the federal government.[125] This is counterintuitive, as the overwhelming, constantly-evolving cybersecurity landscape threatens the entire economy on a national scale; thus, it should be addressed by the federal government, which has the resources, expertise, and personnel to stay ahead of moving targets.

The 115th Congress finally enacted a bipartisan bill in August 2018 that promised to have a positive impact on small businesses by offering cohesive cybersecurity guidelines. The bill is known as the National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act.[126] NIST was born from the Cybersecurity Enhancement Act of 2014, a bipartisan initiative passed by the 113th Congress that enabled the director of NIST to work with entities in the private sector to streamline cybersecurity

120. *See* Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014); Brett V. Newman, Note, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 U. ILL. J.L. TECH. & POL'Y 437, 449 (2015).

121. *See* Newman, *supra* note 120, at 449.

122. *See id.*

123. *See id.*

124. *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012); Jennifer Rizzo, *Cybersecurity Bills Fail in Senate*, CNN (Aug. 2, 2012, 4:19 PM), https://www.cnn.com/2012/08/02/politics/cybersecurity-act/index.html.

125. *See* Rizzo, *supra* note 124.

126. *See* NIST Small Business Cybersecurity Act, Pub. L. No. 115-236, 132 Stat. 2444 (2018); Kevin Townsend, *NIST Small Business Cybersecurity Act Becomes Law*, SECURITY WK. (Aug. 16, 2018), https://www.securityweek.com/nist-small-business-cybersecurity-act-becomes-law.

guidelines.[127] The NIST Small Business Cybersecurity Act aims to direct accessible minimum data security standards specifically at small businesses.[128] There is great optimism surrounding this law,[129] but it may be misguided. The cybersecurity framework guidelines[130] propagated by NIST fall short of meeting its goal. Although the guidelines help small businesses identify their vulnerabilities,[131] they do not provide such businesses with the informational and financial resources to mitigate them. Further, the NIST Small Business Cybersecurity Act guidelines are not meant to be regarded as law or regulatory requirements, and they do not preempt state-based laws. Instead, these guidelines are simply suggestions for small businesses to establish a strategic cybersecurity scheme.[132] While NIST does offer small businesses cybersecurity training in compliance with its suggested guidelines,[133] it is unlikely that such a program will gain significant traction if it is not required by law.[134]

As evidenced by its failure to enact several proposed cybersecurity bills, Congress has to date addressed only some of the deficiencies impacting small business by creating the SBA.[135] Congress must move past partisan concerns to prioritize the enactment of enforceable federal cybersecurity laws and ensure the viability of small businesses.

The SBA should not be overlooked as a powerful advocate for the federalization of data protection and breach notification laws. As part of the Small Business Reauthorization Act of 1997,[136] the SBA introduced the Historically Underutilized Business Zones (HUBZone) contracting

127. *See* Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014); Fadja Tassey, *Current Topics in Internet Law Data Breach Liability*, SETON HALL U. (2018), http://scholarship.shu.edu/student_scholarship/940; Caleb Skeath, *Congress Passes Five Cybersecurity Bills*, INSIDE PRIVACY (Dec. 12, 2014), https://www.insideprivacy.com/united-states/congress-passes-four-cybersecurity-bills.

128. *See* Townsend, *supra* note 126.

129. *See* Evan Wolff et al., *Finally, Cyber Help for Small Business Is on Its Way*, LAW360 EXPERT ANALYSIS (Oct. 1, 2018), https://www.law360.com/articles/1086244/finally-cyber-help-for-small-businesses-is-on-its-way.

130. *See* NAT'L INST. STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

131. *See New NIST Guide Helps Small Businesses Improve Cybersecurity*, NAT'L INST. STANDARDS & TECH. (Jan. 8, 2018), https://www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity.

132. *See* Townsend, *supra* note 126.

133. *See Training*, NAT'L INST. STANDARDS & TECH. (Nov. 20, 2019), https://www.nist.gov/itl/smallbusinesscyber/training.

134. *See* Townsend, *supra* note 126.

135. *See Federal Cybersecurity Regulations*, CORANET (July 10, 2018), https://www.coranet.com/federal-cybersecurity-regulations.

136. *See The HUBZone Act of 1997: Hearing on S. 208 Before the Subcomm. on Small Bus.*, 105th Cong. (1997) [hereinafter *Hearing on S. 208*].

program.[137] In recognition of the need to grow the small business economy, HUBZone requires that at least 3% of the total value of all federal government contracts be awarded to small businesses.[138] The results have been significant; in 2018 alone, the federal government awarded contracts to small businesses totaling over $9.8 billion.[139]

However, despite its storied successes, the SBA has yet to adequately address the overwhelming threat of cybersecurity's inconsistent legal landscape on small businesses. On its website, the SBA provides general guidelines for small businesses hoping to prevent a data breach, yet the website notably lacks internal resources, an explanation of current law, or standards for small businesses to fully understand and mitigate the risks.[140] As the SBA has done in the past to promote the welfare of small businesses, it should expend additional resources to advocate for small business interests through the federalization of data protection and breach notifications laws.

IV. RECENTLY ENACTED DATA PRIVACY LAWS AND SMALL BUSINESSES

The state-based legal approach to data privacy is only growing more convoluted. Recently, certain states have enacted additional data privacy laws following the European Union's (EU) enactment of the General Data Protection Regulation (GDPR) in early 2018. Unlike data breach notification laws, GDPR adopts a "Privacy by Design" approach and addresses the security as well as the affirmative control of each EU resident's personal data, even before a breach can occur.[141] GDPR has applicability worldwide; any business in any country must not only explicitly inform its EU resident consumers of the type of data being collected but also obtain each consumer's affirmative consent to collect that data.[142]

Similar to the "Privacy by Design" structure used by GDPR, California followed suit by enacting the California Consumer Privacy Act (CCPA) in

137. *See* U.S. SMALL BUS. ADMIN., HUBZONE QUICK FACTS 2 (2012), https://www.sba.gov/sites/default/files/files/HUBZone%20Quick%20Facts-1.pdf; HUBZone Program, 13 C.F.R. § 126 (2019); *see also Hearing on S. 208*, *supra* note 136.

138. *See* 15 U.S.C. § 644(g)(1)(A)(iii) (2018); *see also* HUBZONE QUICK FACTS, *supra* note 137.

139. *See* CONG. RESEARCH SERV., SMALL BUSINESS ADMINISTRATION HUBZONE PROGRAM (2019), https://fas.org/sgp/crs/misc/R41268.pdf.

140. *See Small Business Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity (last visited Dec. 30, 2019).

141. *See* Danny Palmer, *What is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know.

142. *See GDPR Key Changes*, EUR. UNION GDPR, http://web.archive.org/web/20181012205054/https://eugdpr.org/the-regulation (last visited Oct. 12, 2018).

May 2018,[143] which provides consumers with affirmative rights over whether their data can be collected and for what purposes it can be used.[144] The CCPA is in effect as of January 2020.[145]

The CCPA was hastily enacted to prevent a stricter California ballot initiative from enactment, and although amended,[146] there remain several deficiencies and vague provisions with unknown impact.[147] The CCPA's applicability is defined in generalized terms and requires that companies conducting business in California provide California consumers with the ability to "opt out" of data collection, including personal information, which involves an undefined "olfactory" information restriction.[148] Further, the CCPA is the first law of its kind to grant California residents a private right of action to bring lawsuits against businesses that allegedly violate its provisions.[149]

As each of the states followed California's lead to enact data breach notification statutes, they are likely to do so again with the CCPA. If each state enacts its own law, state-specific nuances and penalties will further challenge small business compliance.[150] Further aggravating the issue is that some states may mirror California's private right of action provision while others may not. This would force small businesses to decipher complex enforcement provisions with limited resources. Small businesses in such circumstances may realize stunted growth and evade compliance with the laws of each state, ineffectively attempt compliance, or decide not to do business with certain states. Each approach will either cause a financial risk to the business if there is a data breach or may deter business owners from running small businesses at all.

143. *See* California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–.199 (Deering, LEXIS through 2020 Sess.); *The California Consumer Privacy Act of 2018*, CAL. OFF. ATT'Y GEN. (Nov. 17, 2017), https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf; Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill.

144. *See* Palmer, *supra* note 141.

145. *See California Consumer Privacy Act: A Rapid Q&A*, DAVIS WRIGHT TREMAINE LLP (June 29, 2018), https://www.dwt.com/California-Consumer-Privacy-Act-A-Rapid-QA-06-29-2018.

146. *See The CCPA Amendments that Survived the California Legislature*, JONES DAY (Sept. 2019), https://www.jonesday.com/en/insights/2019/09/the-ccpa-amendments-that-survived.

147. *See* Peter Pizzi, *Possible Defects in California's New Privacy Law*, LAW360 (July 30, 2018), https://www.law360.com/articles/1067951/possible-defects-in-california-s-new-privacy-law.

148. *See* CAL. CIV. CODE § 1798.140 (Deering, LEXIS through 2020 Sess.); Odia Kagan, *Does the California Privacy Act Apply to Me?*, FOX ROTHSCHILD LLP (May 15, 2019), https://www.foxrothschild.com/publications/does-the-california-consumer-privacy-act-apply-to-me.

149. *See An Update on the California Consumer Privacy Act and Its Private Right of Action*, JDSUPRA (Sept. 13, 2018), https://www.jdsupra.com/legalnews/an-update-on-the-california-consumer-13743; *The California Consumer Privacy Act of 2018*, *supra* note 143.

150. *See* Pizzi, *supra* note 147.

V. ADDRESSING THE ISSUES: THE NEED FOR A COMPREHENSIVE APPROACH TO DATA PROTECTION AND BREACH NOTIFICATION LAWS

It is financially more feasible for small businesses to comply with one set of rules governing data protection and breach notification. The standardization of minimum security requirements and proportionate penalties for breach will enable small businesses to better assess and plan for risks. Additionally, a consistent set of laws provides consumers with the benefit of better understanding their rights and privileges when they transact with a business.

Proposed solutions, other than a comprehensive federal approach to the dilemmas currently facing small businesses, are fatally flawed.[151] Some argue that data breach insurance should sufficiently cover small business liability for penalties resulting from a breach, therefore ensuring a small business can survive the imposition of such penalties.[152] However, a data breach insurance policy is likely insufficient to cover every instance of breach because each state has specific, ever-evolving requirements. Additionally, many policies contain coverage exclusions for state-imposed regulatory penalties and litigation costs.[153] Thus, a small business that obtains data breach insurance to avoid the financial ramifications of significant penalties and costs in the event of a breach may actually be required to pay those penalties and costs, *in addition to* policy premiums. Further, data breach insurance does not prevent damage to consumers and small business—it simply compensates the damage. A small business' reputation is equally important, and the loss of consumer confidence alone following a breach can cripple a formerly successful small business.

Others have suggested burden-shifting the onus of small business cybersecurity to the credit card companies with which they work.[154] Burden-shifting the responsibility to credit card companies does not protect small businesses because major credit card companies are not incentivized to work with smaller businesses from the onset. Additional liability and security obligations on credit card companies may cause those companies to stop

151. *See, e.g.*, Selznick & LaMacchia, *supra* note 15, at 249 (suggesting a burden-shifting approach); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 432 (2018) (suggesting that data breach insurance is adequate to manage the risks associated with data breach).

152. *See* Talesh, *supra* note 151; Penelope N. Lazarou, *Small Businesses and Identity Theft: Reallocating the Risk of Loss*, 10 N.C. BANKING INST. 305, 325 (2006).

153. *See* Michelle A. Reed et al., *Issues to Consider When Evaluating Cyber Coverage in Light of the CCPA and Other State Privacy Laws*, AKIN GUMP STRAUSS HAUER & FELD LLP: AG DATA DRIVE (Nov. 4, 2019), https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/issues-to-consider-when-evaluating-cyber-coverage-in-light-of.html.

154. *See* Selznick & LaMacchia, *supra* note 15, at 249.

working with small businesses altogether.[155] Indeed, credit card companies have continually imposed the burden of data protection on small businesses.[156] If credit card companies and other financial institutions refuse to work with small businesses, then small businesses cannot thrive.[157]

For the foregoing reasons, a federal standard is necessary. A comprehensive federal approach to data protection and breach notification laws should be inclusive of businesses of all sizes and income levels allowing for a better understanding of the rules, better consumer data protection, and little room for noncompliance.

VI. CONGRESS MUST ENACT A COMPREHENSIVE, MULTI-TIERED FEDERAL SCHEME

The federal government must roll out and implement an overarching data protection and breach notification policy in stages. Congress must first enact a temporary provision that streamlines state laws into one consistent law by which all businesses must temporarily abide while Congress drafts a detailed federal framework. Congress should adopt the provisions of the strictest state-based breach notification law as to the timing requirements of breach notification, the penalties per record breached, and the specificity by which that law defines terms such as "personal information." California's breach notification law is a sufficiently strict law for temporary enactment, as it is known to be restrictive and pro-consumer.[158] Additionally, most of the state-enacted data privacy and breach notification laws have been modeled, at least in part, on this California law.[159] Once adopted, this law should temporarily preempt[160] all other current state laws until businesses can adapt to the requirements of a new federal framework within twenty-four months of its

155. *See, e.g.*, Tony Payne, *Payment Card Industry is Shifting Liability to Merchants*, INSURETRUST, https://www.insuretrust.com/payment-card-industry-shifting-liability-merchants/ (last visited Feb. 28, 2020) (discussing credit card companies' imposition on merchants to adapt credit card chip technology "to shift the liability for data breaches back on retailers who do not adopt sensible and available security technology. Should a data breach occur, the consequences for non-compliant businesses who choose to forgo the liability protection of the card issuers could mean the end of their enterprises").

156. *See, e.g.*, *id.*; Ydstie, *supra* note 9.

157. NAT'L SMALL BUS. ASS'N, 2017 YEAR-END ECONOMIC REPORT 11 (2018), https://nsba.biz/wp-content/uploads/2018/02/Year-End-Economic-Report-2017.pdf (displaying statistics detailing the small business consequences of lacking adequate financing).

158. *See* Alan S. Wernick, *Data Theft and State Law: When Data Breaches Occur, 34 States Require Organizations to Speak Up*, AHIMA HIM BODY KNOWLEDGE (Dec. 2006), http://library.ahima.org/doc?oid=68170#.W9JkdhNKg0o.

159. *See* Lee, *supra* note 48, at 143.

160. *See* Jacob E. Gersen, *Temporary Legislation*, 74 U. CHI. L. REV. 247, 247 (2007) ("An overwhelming portion of legislation enacted by the United States Congress is actually what might be termed temporary legislation—statutes containing clauses limiting the duration of their own validity.").

congressional passage.[161] Although this approach may make certain provisions more difficult to adhere to overall, all businesses will better be able to implement cybersecurity protections and assess their data security risks based upon one set of definitions, rules, and penalties.

When Congress drafts the overarching federal framework for data protection and breach notification law, it must comprehensively take into consideration data breach notification and minimum data protection standards based upon the size of a business, its annual revenue, and the implementation of minimum security requirements based upon the type of data being collected and retained. For example, minimum security standards may be scaled down for a small business retaining PII compared to a large business retaining both PII and PHI, because the large business has access to more resources than a small business and retains more than one type of protected data. Congress should also measure its basis for minimum data security standards around whether data is encrypted, because most state-enacted statutes consider the breach of encrypted data to be an area of safe harbor.[162] Ultimately, the new federal framework must include an express preemption[163] provision to overcome state laws.

The new law should be divided into three tiers: small business (as defined by the SBA), medium business, and large business. Under those tiers, additional tiers based on industry and data types should reveal clear requirements to achieve minimum security standards and include relevant breach notification penalties and remediation regulations. Large compliance departments and independent business owners alike should be able to read, understand, and comply with the rules imposed on them.

Finally, Congress should appoint a new administrative organization to govern and enforce the new federal framework with the assistance of the SBA to ensure that small business interests are represented in the new governance structure. Technology is rapidly evolving, and an efficient way to ensure that the current federal laws are up to date with regard to certain risks is to have

161. In June 2018, The California Consumer Privacy Act was passed and imposed business compliance with its provisions by January 2020, just eighteen months later. *See* John Stephens, *California Consumer Privacy Act*, AM. BAR ASS'N GROUPS: BUS. & CORP. COMM. NEWSL. (July 2, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9.

162. *See* Lee, *supra* note 48, at 147; *see, e.g.*, COLO. REV. STAT. § 6-1-716(1)(h) (LEXIS through 2019 Legis. Sess.) ("'Security breach' means the unauthorized acquisition of unencrypted computerized data . . . ."); N.J. STAT. ANN. § 56:8-161 (LEXIS through 218th 2nd Annual Sess.) ("'Breach of security' means unauthorized access to electronic files . . . containing . . . personal information when access to the personal information has not been secured by encryption . . . ."); FLA. STAT. ANN. § 501.171(1)(g)(2) (LEXIS through 2019 Legis. Sess.) ("The term [personal information] also does not include information that is encrypted . . . .").

163. The Supreme Court recognizes express federal preemption "when Congress includes in a statute explicit language stating an intent to preempt conflicting state law." *See In re* Anthem Data Breach Litig., 162 F. Supp. 3d 953, 1013 (N.D. Cal. 2016) (quoting Deweese v. Nat'l R.R. Passenger Corp. (Amtrak), 590 F.3d 239, 245 (3d Cir. 2009)).

a dedicated committee working on amendments to the law. Additionally, the establishment of one centralized entity that consumers, small businesses, and large businesses can contact ensures a relatively predictable enforcement process. This method of governance and enforcement should preempt all others.

CONCLUSION

Small businesses are the driving force of a healthy American economy. However, their limited financial and technological resources make it difficult to comply with and endure the penalties under current data protection and breach notification laws. Disjointed state-based and limited federal data laws overwhelm small businesses and put them at a high risk of failure. The enactment of recent data privacy laws potentially exacerbates that risk.

Proposed solutions, such as burden-shifting cybersecurity liability and promoting data breach insurance, do not fully address the risks to small businesses. To encourage the success of small businesses, Congress must examine current laws to create a comprehensive data protection and breach notification federal framework that preempts state-based laws, simplifies compliance, and centralizes enforcement.

Nadia Udeshi[*]

* B.Des., The Pennsylvania State University, 2007; J.D. Candidate, Brooklyn Law School, 2021. To the staff and editors of the Brooklyn Journal of Corporate, Financial & Commercial Law, thank you for all of your efforts in preparing this Note for publication. To my parents, Lachman and Vimla Udeshi, thank you for your support. To my husband, Jordan Yanco, thank you for everything that you do and are – this Note is dedicated to you.