CCPA TIPPING THE SCALES: BALANCING INDIVIDUAL PRIVACY WITH CORPORATE INNOVATION FOR A COMPREHENSIVE FEDERAL DATA PROTECTION LAW

SAHARA WILLIAMS*

I. INTRODUCTION

Over the past ten years, reported data breaches in the U.S. have increased from 656 breaches, exposing 35.7 million records, to 1,244 breaches, exposing 446.52 million records, at the end of 2018.[1] Doing the math, that is more than ten times the stolen records per breach, indicating hackers are getting more efficient.

Forty-six percent of breaches in 2018 targeted the general business sector, accounting for a staggering ninety-three percent of exposed records.[2] The impact on U.S. businesses has been significant by damaging the brand reputation and impacting consumer trust and satisfaction.[3] Organizations reported losing an average of $5.7 million when their customer base dropped by four or more percent due to security breaches.[4] Even organizations affected by data breaches that were, for the most part, able to maintain customer loyalty suffered an average loss of $2.8 million.[5]

The cost of data protection is skyrocketing due to expenses from upgrading security measures, conducting breach response activities, and litigating liability. Reported data breach response costs were up 1.5% for the first four months of 2019 over the previous year.[6] The average response cost per record is $150, and total average response costs are $3.92 million.[7] While businesses reported that more than fifty percent of data breach expenses amassed within a year of the data breach discovery, more than ten percent of costs accrued more than two years

---

* Sahara Williams is a practicing engineer, fourteen-year entrepreneur, and 2020 Juris Doctor candidate at the Indiana University Robert H. McKinney School of Law focused on Intellectual Property Law.

1. J. Clement, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018 (in Millions)*, STATISTA (Aug. 5, 2019), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://perma.cc/FF44-95EE].

2. *2018 End of Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER 9 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf [https://perma.cc/E7FY-L6RN]. "Business Sector" includes retail, hospitality, professional, trade, transportation, utilities, payment processors, nonprofits, non-medical insurance, and other businesses not considered to be financial, educational, healthcare, or government.

3. *See Cost of a Data Breach Report 2019*, IBM SECURITY 3 (2019), https://www.ibm.com/downloads/cas/ZBZLY7KL [https://perma.cc/MF6U-H684].

4. *Id.*

5. *Id.*

6. *Id.* at 18.

7. *Id.* at 3.

after the breach.[8]

The interest in data protection is not just about mitigating financial losses for businesses. Many "bad actors" in cybersecurity and data analytics are foreign nationals or state-sponsored terrorists seeking to compromise U.S. national security, gain advances in international relations, or even influence U.S. elections and political views.[9] U.S. data protection vulnerabilities span the private and public sectors,[10] and the strong interplay between the two creates joint liability and responsibility to address the issues.

While consumers generally face a lower financial burden than businesses, the impact of weak data protection laws can be devastating to consumers. When there is a data breach, consumers can become victims of identity theft, financial loss, jeopardized credit ratings, compromised personal privacy, and health record theft.[11] Reported consumer losses due to identity theft were $16.8 million in 2017,[12] and Federal Trade Commission records show an increase to $1.48 billion in 2018.[13]

The economic impact of cyber hacking, the threats to national security, and the effect on consumers all demand that the United States focus on improving data protection. The question is, how should it be done? The federal government has focused on securing high-risk industries while state governments have mostly enacted consumer notification laws, and businesses have worked to better secure their networks.[14]

Consumers, though, have started demanding a greater emphasis on data

---

8. *Id.* at 5.

9. *American Bar Association Cybersecurity Legal Task Force Report to The Board of Governors Resolution*, CITY BAR CTR. FOR CONTINUING LEGAL EDUC. (May 9, 2014), available at 2014 WL 2921323 [hereinafter *Cybersecurity Legal Task Force*].

10. *Id.*

11. *How Common Is Identity Theft? (Updated 2018) The Latest Stats*, LIFELOCK (last updated Apr. 13, 2018), https://www.lifelock.com/learn-identity-theft-resources-how-common-is-identity-theft.html [http://perma.cc/ZGW4-SEPB].

12. *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study*, JAVELIN STRATEGY & RESEARCH (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin# [http://perma.cc/S96R-S89J].

13. Rob Douglas, *2019 Identity Theft Statistics: Trends and Statistics About Identity Theft*, CONSUMERS AFFAIRS (June 21, 2019), https://www.consumeraffairs.com/finance/identity-theft-statistics.html [https://perma.cc/N5ZB-DWRT].

14. Gregory J. Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 194 (2015); *see also* Deborah Thoren-Peden & Catherine Meyer, *Data Protection 2018: USA*, INT'L COMP. LEGAL GUIDES (Dec. 6, 2018), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [http://perma.cc/WPU6-KVVU] (discussing business autonomy in cybersecurity).

privacy.[15] While Congress has proposed many failed data privacy measures,[16] state governments have started to act. California led the way with the passage of the Consumer Privacy Act of 2018 ("CCPA").[17] Many believe the CCPA is serving as the tipping point for business sector support of a comprehensive federal data protection law in the United States.[18]

This Note proposes enactment of a comprehensive federal data protection law that recognizes and balances individual privacy rights, enacts minimum cybersecurity standards, simplifies security breach responses, and increases efficiency in compliance and enforcement of cyber laws. Section II defines comprehensive data protection. Section III provides an overview of U.S. data protection laws. Section IV summarizes the momentum towards federal data privacy legislation. Section V identifies and analyzes alternative data protection approaches. Section VI proposes a comprehensive solution for improving data protection, and the components of the recommended comprehensive federal data protection law are summarized in Section VII.

II. COMPREHENSIVE DATA PROTECTION DEFINED

Comprehensive data protection is composed of three categories: (1) information or data privacy, (2) cybersecurity or data security, and (3) breach response. The privacy category includes the ownership, access, collection, and deletion of data. The security category includes the safekeeping, maintenance, and sharing of data. The response category includes notification, compensation, and penalties in case of a breach.[19]

The issues that arise between consumers and corporations in data protection can be analogized as a tenant-landlord relationship. Imagine that a consumer, which could be an individual or a business, wants to lease an apartment or office from the corporation that owns the building. The consumer contacts the corporation to lease the space and moves personal belongings into the leased space. Below are the privacy, security, and notification issues that stem from this scenario.

From a privacy perspective, has the consumer given the corporation ownership of the personal belongings placed in the space; does the corporation have a license to freely use the personal belongings in the space; when and for what reasons can the corporation access the space; and does the corporation have to get permission to access the space or tell the consumer that the space was accessed?

---

15. *See infra* notes 70, 71 (discussing the consumer outcry after Facebook announced the misuse of user information).

16. *See infra* notes 86, 90 (giving examples of some failed data protection measures).

17. CAL. CIV. CODE § 1798.100 (2018).

18. *See infra* Section IV (discussing the momentum towards data privacy protections).

19. *See* Stephen P. Mulligan, Chris D. Linebaugh & Wilson C. Freeman, *Data Protection and Privacy Law: An Introduction*, CONGRESSIONAL RESEARCH SERVICE (May 9, 2019), https://fas.org/sgp/crs/misc/IF11207.pdf [https://perma.cc/E46L-8TKJ].

As it relates to security, does the corporation have to provide security for the space; if so, what level of security might the corporation have to provide–a lock, an alarm, or a security camera; and can the corporation allow its vendors or contractors into the space?

Finally, if the space is broken into, what should the corporation's response obligations be? For instance, does the corporation have to notify the consumer; for what does the corporation have to compensate the consumer–the loss of security, stolen items only, or stress related to the break-in; and finally, should the government sanction the corporation as well?

While these questions may be straightforward to answer when dealing with the physical relationship between a tenant and a landlord, the answers are less clear-cut in the digital relationship between consumers and corporations. Landlords do not generally need access to a tenant's personal belongings, but a healthcare corporation cannot provide healthcare services without accessing and using a consumer's data. Security for an apartment is typically sufficient if the apartment has a lock and an alarm. In the digital world, hackers are continuously developing new ways to steal consumer data requiring businesses to be on constant guard. Theft of a television is easy to notice, quantify, and replace. But it may take days, weeks, or even months to detect that hackers copied digitized information. That information may be used to steal money from the consumer or may not be used at all, making it difficult to quantify consumer damages. By addressing privacy, security, and breach response matters, data protection laws shelter digitized consumer information, specify safekeeping measures, and clarify the responsibilities of consumers, corporations, and third parties.

III. DATA PROTECTION IN THE UNITED STATES

While data protection has three categories, it is holistically about controlling and securing private information. Historically, privacy has been considered fundamental in U.S. society. Samuel Warren and Louis Brandeis popularized the phrase "the right to be let alone" in their 1890 law review article.[20] Since then, the U.S. Supreme Court has recognized the right to privacy in many contexts.[21] Several torts have been used to protect the physical privacy of individuals, including public disclosure of private facts, intrusion upon seclusion, false light, appropriation, breach of confidentiality (by professionals), defamation, infliction of emotional distress, and trespass.[22]

---

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

21. *E.g.*, Eisenstadt v. Baird, 405 U.S. 438 (1972) (acknowledging marital privacy); Whalen v. Roe, 429 U.S. 589 (1977) (acknowledging privacy regarding medical records); Smith v. Org. of Foster Families for Equal. and Reform, 431 U.S. 816 (1977) (acknowledging family privacy as a human right); *see also* Jugpreet Mann, Note, *Small Steps for Congress, Huge Steps for Online Privacy*, 37 HASTINGS COMM. & ENT. L.J. 365 (2015) (summarizing Warren & Brandeis, *supra* note 19).

22. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 32-33 (Wolters

As the conversation about privacy has moved from the physical world to a digital construct, the consumer's right to privacy has been less certain. The first cyber-attack was reported in 1988 when a Cornell graduate student hacked Massachusetts Institute of Technology's network.[23] Today, the judicial branch has declined to extend traditional privacy protections to digitized information.[24] The legislative response to digital privacy concerns has resulted in a hodgepodge of laws at the federal and state level. Each law defines and regulates data privacy, data security, and breach response requirements in different ways that in some cases diverge and in other cases overlap.[25]

A. Federal Level Data Protection

The United States has more than twenty federal data protection laws that address cyber protections in varied and inconsistent ways.[26] Federal laws primarily focus on the security category but only for certain sectors. These sector-specific laws focus on shielding certain classes of information like medical records under the Health Insurance Portability and Accountability Act ("HIPAA") and financial transactions under the Gramm-Leach-Bliley Act ("GLBA").[27]

Federal enforcement of data protection laws is spread out between multiple agencies,[28] but the Federal Trade Commission ("FTC") does the heavy lifting.[29] Section 5 of the FTC Act bans "unfair or deceptive acts or practices in or affecting [interstate or foreign] commerce,"[30] and in 2014, a federal court held

---

Kluwer, 6th ed. 2018).

23. Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L. J. 217, 220-21 (2016) [hereinafter *Bottoms Up*].

24. Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 466-67 (2016) (discussing the challenges of using tort and contract laws to protect consumer privacy, a corporation's use of the First Amendment to gain judicial support for its right to use consumer data, and the judicial findings of no cognizable injury to consumers under tort law); *see also* Charles Cresson Wood, *Solving the Information Security & Privacy Crisis By Expanding the Scope of Top Management Personal Liability*, 43 J. LEGIS. 65, 91 (2016) (explaining that individuals do not own their personal information in the U.S.).

25. *See* Evans, *supra* note 14.

26. *Data Protection Laws of the World: United States*, DLA PIPER (last modified Jan. 28, 2019), https://www.dlapiperdataprotection.com/index.html?c=US&c2=GB&go-button=GO&t=law [http://perma.cc/J46A-TDU3].

27. SOLOVE & SCHWARTZ, *supra* note 22, at 773.

28. *Bottoms Up*, *supra* note 23, at 221 (discussing enforcement efforts by the Department of Homeland Security, National Security Agency, Department of Defense, and FTC).

29. Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 446 [hereinafter *When Toasters Attack*].

30. Evans, *supra* note 14, at 201 (quoting 15 U.S.C. § 45(a)(1) (2012)).

that the FTC Act is inclusive of corporate cybersecurity practices.[31] Under its powers, the FTC has sought to ensure companies "maintain reasonable and appropriate data security practices" and enforce the published policies of major companies.[32] However, the proof required to show "unfair or deceptive" practices is somewhat subjective and difficult to prove in industries where there are not strong federal laws in place.[33] Consequently, industries outside of healthcare, finance, and a few other specialized areas do not face consistent prosecution for violations of the FTC Act.[34] Moreover, technology is rapidly changing, and it is unclear whether courts will continue to extend the FTC's authority over new legal challenges.[35] This uncertainty leaves gaps in the protection provided by the FTC and uncertainty as to the long-term viability of the protections offered.

This patchwork policy has not only left gaps in cyber protections, but it has also frustrated international commerce.[36] The European Union has long been seen as the global leader in data protection policies.[37] This reputation was strengthened when the General Data Protection Regulation ("GDPR") went into effect in 2018.[38] The GDPR covers more than forty European countries,[39] and other countries are following the E.U.'s lead.[40] Under the GDPR, the E.U. evaluates the data protection measures of companies seeking to do business with European residents.[41] The perception of U.S. laws lacking data privacy protections is

---

31. *Id.* at 188 (summarizing the holding in F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 615 (D.N.J. 2014)).

32. *Id.*; *see also* Fairclough, *supra* note 24, at 467.

33. *When Toasters Attack*, *supra* note 29, at 446; *see also supra* Section III.A (providing examples of federal sector-based laws).

34. *When Toasters Attack*, *supra* note 29, at 447.

35. Evans, *supra* note 14, at 189-91 (discussing the fragility of the FTC's authority).

36. *See generally* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000) (discussing the tension between the U.S. and E.U. as it relates to data protection).

37. Morgan A. Corley, Note, *The Need for an International Convention on Data Privacy: Taking a Cue from the CISG*, 41 BROOK. J. INT'L L. 721, 726-27 (2016).

38. Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L. 119) 1.

39. Laurie Beasley, *Do You Know Which Countries are Included in GDPR Compliance?*, BEASLEY DIRECT AND ONLINE MARKETING, INC. (June 12, 2018), https://beasleydirect.com/gdpr-countries/, [https://perma.cc/QKZ3-GU2U] (listing the countries covered by the GDPR).

40. Katie Yahnke, *A Practical Guide to Data Privacy Laws by Country*, I-SIGHT (Nov. 5, 2018), https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/ [http://perma.cc/EFH9-84YX] (discussing global privacy laws, including new efforts in Brazil, India, and China).

41. *Adequacy of the protection of personal data in non-EU countries*, EUROPEAN COMM'N (accessed Oct. 9, 2018), https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en [http://perma.cc/A5WL-A9EJ].

bringing greater scrutiny to U.S. businesses and is complicating international trade negotiations.[42]

B. State-Level Data Protection

While federal laws are helpful for the limited industry groups they cover, many gaps in data protection subsist throughout the broader business sector.[43] State laws cannot adequately fill these gaps because who and what the laws cover varies significantly.[44] For example, the California Online Privacy Protection Act of 2003 ("CalOPPA") requires website owners to disclose privacy practices,[45] and the California Consumer Privacy Act of 2018 institutes privacy rights that rival the GDPR.[46] But the California protections only apply to consumers who are California residents.[47]

Most state regulations regarding cybersecurity consist of general statements that data should be secured.[48] However, some states have gone further. Massachusetts, for instance, has regulations for data encryption, network security, employee training, and third-party data sharing,[49] and Ohio's new cyber law seeks to protect businesses that institute minimum security requirements.[50]

All states have enacted breach response notification laws.[51] Enforcement of state data protection laws is a function of each state's Attorney General's office.[52] Grounds for criticizing state laws include not always requiring the breached company to provide credit monitoring to affected consumers, not allowing for private causes of action, and not issuing penalties sufficient to incentivize

---

42. *See generally* Shaffer, *supra* note 36.

43. Thoren-Peden & Meyer, *supra* note 14.

44. *Id.*

45. Sara Pegarella, *CCPA versus CalOPPA*, TERMSFEED (Dec. 2, 2018), https://termsfeed.com/blog/ccpa-vs-caloppa/ [http://perma.cc/LE4J-TZUF]; *see also* Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575-79.

46. *See infra* Section V.A (discussing the GDPR and CCPA privacy provisions).

47. Pegarella, *supra* note 45.

48. For example, Indiana law states: "A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner." IND. CODE § 24-4.9-3-3.5(c) (2018).

49. Margaret Rouse, *Massachusetts data protection law*, TECHTARGET (Jul. 2009), https://whatis.techtarget.com/definition/Massachusetts-data-protection-law [https://perma.cc/QY8X-HUJV].

50. *See infra* notes 172-80 and accompanying text (discussing the Ohio Law).

51. Jeewon Kim Serrato, Chris Cwalina, Anna Rudawski, Tristan Coughlin, & Katey Fardelmann, *US States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT (Jul. 9, 2018) (discussing US data protection laws including that all 50 states have breach notification law), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/ [http://perma.cc/NQC6-HZTV].

52. Evans, *supra* note 14, at 213 (discussing Attorney General roles in data protection).

businesses to strengthen security.[53]

C. Private Data Protection Efforts: The NIST Framework Example

Data protection is not just a focus of the government. The business sector has been working to stop data hacks and improve cybersecurity.[54] Due to the gaps in federal and state laws, most businesses are only subject to the security measures they impose on themselves.[55] Many businesses have responded by implementing company-specific cybersecurity policies[56] or collaborating with the government and industry groups to develop best practices for voluntary use.[57]

The National Institute for Standards and Technology ("NIST") developed one such collaboration, which consists of the 2014 NIST Framework followed by the 2015 Framework for Cyber-Physical Systems (collectively, "NIST Framework").[58] The NIST Framework professes to be a regularly updated best-practice guideline for data security measures.[59] The NIST Framework is not a replacement of any particular cybersecurity measure but rather a means to "identify, implement, and improve cybersecurity practices" as well as create a common "language" within the cybersecurity industry to facilitate communication and issue resolution.[60] Adding to its benefits, NIST collaborates with more than twenty foreign countries, including the United Kingdom, Japan, and Germany and thus has the potential to be a global standard in cybersecurity.[61]

The NIST Framework and other security frameworks are emerging as a defense in negligence and tort claims to show that a reasonable standard of care was met.[62] Critics call the NIST Framework reactionary.[63] The NIST Framework is more of a risk assessment tool than a minimum standard and allows a corporation to choose what level of security it desires.[64] The concern is that the

---

53. *See generally* STEPHEN Y. CHOW, *Survey of State Data Security and Privacy Law*, *in* DATA SECURITY AND PRIVACY IN MASSACHUSETTS, ch. 9 (2d ed. 2018) (discussing the differences in various state data protection laws).

54. Corley, *supra* note 37, at 743-44 (discussing tech company enhancements to cybersecurity).

55. Thoren-Peden & Meyer, *supra* note 14 (discussing business autonomy in cybersecurity).

56. *Bottoms Up*, *supra* note 23, at 218 (describing the business-led approach).

57. Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L. J. 1029, 1042 (2013).

58. *When Toasters Attack*, *supra* note 29, at 441-43.

59. *Bottoms Up*, *supra* note 23, at 219.

60. *When Toasters Attack*, *supra* note 29, at 442.

61. *Id.*

62. *Id.* at 443 (discussing duty of care in negligence and recklessness claims for data breaches).

63. *Id*. at 441.

64. *Bottoms Up*, *supra* note 23, at 223-25 (explaining how the NIST Framework is used by a business to compare its practices with "best" practices, assess how risk resistant its systems are, and create a plan to improve its security to a self-determined target level).

NIST Framework evaluates the business' risk, not the consumers'. Still, it is an example of a collaborative effort between the private sector and government to establish best practices in cybersecurity.

IV. THE SCALES HAVE TIPPED: DEMAND FOR DATA PRIVACY AS A PART OF DATA PROTECTION

As the use of the internet has increased, so too have the calls for increased data privacy. Globally, more than 150 countries have included a right to privacy in their constitution,[65] and more than forty countries have implemented new consumer privacy regulations.[66] The United Nations has taken note and created a designated position to lead its efforts in global privacy rights.[67]

In the U.S., regulations in the security and response categories have been enacted, but the slow federal reaction to privacy concerns has left Americans without a baseline of data protection.[68] "Privacy concerns stem from breaches and abuse in the collection, storage, transfer, and use of this uniquely identifiable information."[69] Consumer outrage was sparked in 2018 when Facebook revealed that European-based Cambridge Analytica acquired the personal information of eighteen million Facebook users and subsequently used that information in deceptive activities related to the 2016 U.S. presidential election.[70] California consumers responded to this revelation by forcing passage of the CCPA.[71] Many experts predicted that other states would follow California's lead,[72] and so they

---

65. Wikipedia, *Right to Privacy*, WIKIMEDIA FOUNDATION, INC. (updated Oct. 12, 2018) (referencing *Right to Privacy*, CONSTITUTE PROJECT (accessed Oct. 9, 2018), https://www.constituteproject.org/search?lang=en&key=privacy [http://perma.cc/R3R7-FYJN]), https://en.wikipedia.org/wiki/Right_to_privacy [http://perma.cc/KJ79-P39A].

66. *Supra* Section III.A (discussing the enactment and coverage of the GDPR and similar laws).

67. *UN: Major Step on Internet Privacy*, HUMAN RIGHTS WATCH (Mar. 26, 2015), https://www.hrw.org/news/2015/03/26/un-major-step-internet-privacy [http://perma.cc/62RZ-M7FV].

68. *Supra* Sections III.A-B (discussing federal and state level U.S. data protection laws and the focus on cybersecurity and breach response measures).

69. Sunni Yuen, *Exporting Trust with Data: Audited Self-Regulation As A Solution To Cross-Border Data Transfer Protection Concerns In The Offshore Outsourcing Industry*, 9 COLUM. SCI. & TECH. L. REV. 41, 2 (2008).

70. Cecilia Kang & Sheera Frenkel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html [http://perma.cc/G85L-ZNMV].

71. Issie Lapowsky, *The Fight Over California's Privacy Bill Has Only Just Begun*, WIRED (Aug. 29, 2018) (explaining that the CCPA was passed only after Californians for Consumer Privacy led a voter initiative to get a privacy law on the ballot), https://www.google.com/amp/s/www.wired.com/story/california-privacy-bill-tech-lobbying/amp [https://perma.cc/HJU5-X5CK].

72. Forbes Technology Council, *How Will California's Consumer Privacy Law Impact The*

have. While the CCPA is still considered the most comprehensive and far-reaching state data privacy law, privacy and cybersecurity measures are being considered in ten or more states across the country.[73] This onslaught of state regulations means U.S. companies doing business online or across state lines will have to understand, comply with, and stay abreast of hundreds of more laws, each different from the previous.

Consumers are not alone in their call for greater data privacy. The nation's de facto data protection enforcement agency, the FTC, has sought Congressional action to improve data protection since 2012.[74] In addition to the FTC's call for a national data breach notification law[75] and continued support of industry-specific cybersecurity measures,[76] the FTC offered guidance for the development of data protection laws that included minimizing unnecessary data collected by corporations and allowing consumers to choose what data they share.[77] "Companies should build in consumers' privacy protections at every stage in developing their products, including . . . limited collection and retention of [consumer] data and reasonable procedures to promote data accuracy."[78] "Companies should give consumers the option to decide what information is shared about them, and with whom."[79] "Companies should disclose details about their collection and use of consumers' information and provide consumers access to the data collected about them."[80] FTC statements like these, indicating strong support for data privacy reform, are notable because the agency had previously been focused on breach response.

Direct support for privacy regulations has come from recent presidential administrations as well. The Obama administration released its privacy framework when it published the 2012 Consumer Privacy Bill of Rights ("PBOR") based on the Fair Information Practice Principles ("FIPPs").[81] FIPPs

---

Data Privacy Landscape?, FORBES (Aug. 20, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#65e3d75ae922 [http://perma.cc/3K6Q-JQY5] (indicating most of the thirteen-member council believe privacy initiatives will spread quickly across the nation).

73. Cynthia Brumfield, *11 New State Privacy and Security Laws Explained: Is Your Business Ready?*, IDG COMMUNICATIONS, INC. (Aug. 8, 2019), https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html [https://perma.cc/R4TP-2GRB].

74. *When Toasters Attack*, *supra* note 29, at 444 (recounting FTC Chairman Jon Leibowitz's 2012 testimony before Congress encouraging laws that increase the pace of self-regulation).

75. *Id.*

76. *Final FTC Privacy Report Seeks New Laws, Supports 'Do Not Track,' Exempts Small Businesses, and Targets Data Brokers*, CITY BAR CTR. FOR CONTINUING LEGAL EDUC., June 15, 2012, available at 2012 WL 4344717 [hereinafter *Privacy Report*].

77. *When Toasters Attack*, *supra* note 29, at 444.

78. *Privacy Report*, *supra* note 76.

79. *Id.*

80. *Id.*

81. Evans, *supra* note 14, at 198-99.

are international standards for data protection, but they were first proposed by a U.S. government advisory committee in 1973 before becoming the basis for European privacy laws.[82] FIPPs include the principles of notice, access, choice, accuracy, data minimization, security, and accountability.[83] The PBOR asserts the FIPPs' principle of safeguarding consumer privacy as a "'right' owed to consumers and an obligation placed on companies."[84] Moreover, in 2018, the Trump administration announced that the National Economic Council would draft a consumer privacy policy for consideration by Congress.[85]

Congress is aware of the concerns with data privacy, and many of its members have advocated for new laws. Indeed, Congress has produced many failed efforts to protect data privacy.[86] 2019 Congressional efforts to pass a comprehensive federal data protection law appear poised to fail,[87] but piecemeal legislation is being proposed[88] showing a willingness to make some progress. Too, consumer advocacy groups are continuing to pressure the legislature for action.[89]

The legal community, too, has weighed in on federal data privacy laws. The American Bar Association ("ABA") urges five principles for consideration in the development of new data protection laws.[90] While the ABA principles emphasize collaboration between government and the business sector, one of the principles implores that "[p]rivacy and civil liberties must remain a priority when developing cybersecurity law and policy."[91]

The final vote of support for data privacy protections must come from businesses. While many in the technology sector have been resisting privacy regulations in the U.S., other industries want more synergistic policies with

---

82. *Id.*

83. *When Toasters Attack*, *supra* note 29, at 441.

84. Evans, *supra* note 14, at 200 (discussing the inclusion of the FIPPS security principle in multiple government data protection measures).

85. Laura Jehl & Sara M. Goldstein, *Is a New Federal Data Privacy Law on the Horizon? The Tech Industry Sure Hopes So*, 25 No. 09 WESTLAW J. CLASS ACTION 16 (Oct. 16, 2018).

86. Eric Naing, *Hill Panel Urges Stronger Data Security Rules*, CONGRESSIONAL QUARTERLY INC., 2014 CQBNKRPT 0744 (May 15, 2014) (referencing failed data protection bills from Senator Leahy, Senator Thune, Senator McCain, and Senator Kerry).

87. Kiran Stacey, *Senate Talks on US Data Privacy Law Grind to a Halt*, FINANCIAL TIMES LTD (June 11, 2019), https://www.ft.com/content/ecbc11d0-8bad-11e9-a24d-b42f641eca37 [https://perma.cc/6T57-R993].

88. Kathryn Branson, *Federal Consumer Data Privacy Legislation in the 116th Congress*, EDUCAUSE (May 13, 2019), https://er.educause.edu/blogs/2019/5/federal-consumer-data-privacy-legislation-in-the-116th-congress [https://perma.cc/ST5P-2CXR].

89. Justin Antonipillai & John Ackerly, *It's Time for The U.S. to Lead on Data Privacy Law | Opinion*, NEWSWEEK (Mar. 10, 2019), https://www.newsweek.com/its-time-us-lead-data-privacy-law-opinion-1357558 [https://perma.cc/SA6F-EHMS].

90. *Cybersecurity Legal Task Force*, *supra* note 9 (listing in detail the five principles the ABA recommends being included in the development of a federal data protection law).

91. *Id.*

Europe that will facilitate trade.[92] For instance, the Securities Industry and Financial Markets Association and its European counterpart, the Association for Financial Markets in Europe, urged "compatible regulatory regimes" between the U.S. and Europe to facilitate the transcontinental movement of data.[93] In a joint statement, they declared, "Liberalizing trade in financial services is about open markets, clear rules and fair competition, not deregulation."[94]

It seems, though, that enactment of the CCPA is the tipping point toward greater corporate support for federal data privacy protections. In 2018, Facebook and other national technology corporations expressed support for a preemptive federal data protection law, and they have since joined with other technology companies in lobbying for such a measure.[95] Yet the question remains of how data privacy should be integrated into data protection.

V. DECISIONS, DECISIONS: HOW SHOULD WE IMPROVE DATA PROTECTION?

Despite an almost universal consensus on the need to improve data protections, there is not agreement on what those improvements should be. Due to the global nature of today's business climate, some people prefer an international data protection policy over a national policy.[96] They argue that "the global nature of the Internet renders jurisdictional-specific legislation both weak and ineffective."[97] It is difficult to assess under which jurisdiction a legal matter falls when data has crossed multiple jurisdictions, rendering enforcement efforts cumbersome when enforcement is even possible.[98]

Generally speaking, international cooperation and global standards are desirable, but the U.S. must have a national standard first. Creation of a national standard gives due respect to the representative form of government valued so much by Americans.[99] Thus, while there is a need for international collaboration on data protection, the U.S. can ill afford to skip the critical step of developing a national standard first.

This section will describe the main issues in U.S. data protection and analyze

---

92. Fairclough, *supra* note 24, at 468-69 (referencing Facebook's opposition to efforts to create data privacy laws in 2013 and Facebook, Google, and Spokeo's efforts against consumer legal claims to establish harm from data breaches).

93. Randolph Walerius, *Financial Industry Wants U.S.-EU Investment Pact to Open Borders for Business, Data*, CONG. QUARTERLY, INC., Feb. 21, 2013, *available at* 2013 WL 632231.

94. *Id.*

95. Jehl & Goldstein, *supra* note 85; *see also* Stacey, *supra* note 87 and Branson, *supra* note 88.

96. Corley, *supra* note 37, at 746-66 (discussing historical efforts related to international cooperation on data privacy including the Safe Harbor Agreement, the Privacy Shield, the Organization for Economic Cooperation and Development ("OECD"), and the Global Privacy Enforcement Network ("GPEN")).

97. *Id.* at 722.

98. *Id.*

99. *See* Yuen, *supra* note 69, at 73 (discussing American versus European views of privacy).

various approaches for improvement including the demand for consumer privacy, the tension in industry-government interaction, assignment of liability, and special considerations for small businesses.

A. The Privacy Debate: Consumer Versus Industry Control

In developing a national standard for data protection, privacy is the first issue to consider because, ultimately, data protection is about controlling and securing private information. The European Union's General Data Protection Regulation ("GDPR"), which builds on the E.U.'s 1995 General Data Protection Directive ("GDPD"), is widely viewed as the most formative data privacy law in the world.[100] The GDPR model recognizes that "[e]ffective world-wide data protection . . . requires a 'front-end model' solution . . ."[101]

The GDPD established privacy as a fundamental right, placed limits on what and how data is collected, required the deletion of data at an appropriate time, compelled the accurate maintenance of records, made cybersecurity safeguards essential, implemented notification for data collection, and mandated consumer consent for processing personal information.[102]

The GDPR strengthened the GDPD concepts, promulgated them into law, and made them effective against overseas businesses targeting E.U. residents.[103] The main privacy provisions of the GDPR include punitive fines of up to four percent of revenue, opt-in versus opt-out consent–to–collect provisions, seventy-two-hour breach notification, consumer access to collected data, and data deletion upon customer request.[104]

The GDPR has already shown its influence in the United States.[105] The CCPA, which will go into effect on January 1, 2020, is the biggest evidence yet of the GDPR's influence.[106] The main privacy provisions of the CCPA include notification that consumer data is being collected as well as disclosure of how and where data is being collected, the purpose of the data collection, and with whom the data is being shared.[107] Consumers are also granted the right to have their data deleted, and minors under sixteen must opt-in to data collection, while adults have the ability to opt-out without repercussions.[108] Finally, businesses can incentivize consumer consent to data sharing.[109] In addition, an amendment to the

---

100. Corley, *supra* note 37, at 726.

101. Yuen, *supra* note 69, at 38 (discussing the need to include data privacy as a part of data security and data protection efforts).

102. Corley, *supra* note 37, at 727-29.

103. *Id.*

104. Regulation (EU) 2016/679, *supra* note 38.

105. A review of privacy practices of globally operating companies like Facebook, 23andMe, and McDonald's show GDPR provisions have been added for European residents.

106. CAL. CIV. CODE § 1798.100 (2018).

107. *Id.*

108. *Id.*

109. *Id.*

bill clarified the consumer's private right of action for violations of the law.[110]

A key difference between the CCPA and the GDPR is the opt-out versus opt-in provision for consumer consent to data collection. Opt-in rights are key for consumer advocates, especially as it relates to data mining. However, opt-out can be effective for this purpose if notifications are placed conspicuously on websites, the opportunity to opt out is given before the data collection starts, and opting out is a simple process. For example, if a graphic overlay with a "click to opt-out" button was placed over the homepage of a website, consumers would choose to opt-out or continue surfing. The difference between this proposal and the current model is that under the current model, consumers, generally, must search for the privacy policy and opt-out provisions, data collection can begin before the consumer has a reasonable opportunity to opt out, and oftentimes, the consumer has to opt out of multiple third-party sites in addition to the main site. Some websites require a written letter or separate communication to opt out while opt-in is generally a one-click service.[111]

While consumer advocates cheer the protections of the CCPA, some businesses have advocated for a deregulated, consumer-driven, industry-managed approach to privacy. The Trustmark or accreditation approach attempts to keep the management and control of data protection efforts within the business community.[112] Essentially, entrepreneurs would develop data protection compliance certification programs with specific requirements.[113] Corporations that meet the requirements of the program and wish to brand themselves as "certified" would purchase the certification.[114] In theory, customers, then, would gain confidence that the certified corporation adheres to certain privacy standards.[115]

Trustmark advocates lean on market forces and good business strategies to ensure the certification companies act independently and provide value; thus, monitoring the Trustmark industry would be the only role for government in ensuring privacy protections.[116] Such programs have already materialized in response to the enactment of the GDPR.[117] In the U.S., certification of individuals

---

110. *Id.*; *see also* Michael Lamb, *California Legislature Publishes CCPA Amendments; Vote Scheduled For This Week*, INT'L ASS'N OF PRIVACY PROF'LS (Aug. 27, 2018), https://iapp.org/news/a/california-legislature-publishes-cacpa-amendments-vote-scheduled-for-this-week/ [http://perma.cc/66CY-FVYP].

111. *E.g., Privacy Policy*, AFLAC GRP. (Mar. 1, 2019), https://www.aflac.com/about-aflac/privacy-policy.aspx [https://perma.cc/DQP4-N9D9]. Aflac, for example, requires customers to mail in their opt-out notification. Other websites generally list privacy links within the footer of the website that can be navigated to determine the opt-out policy.

112. Yuen, *supra* note 69, at 46.

113. *Id.*

114. *Id.* at 54.

115. *Id.*

116. *Id.* at 46.

117. Two examples of such programs are administered by TÜV Rheinland and Bureau Veritas Group, respectively. *E.g.*, *Product Certification: Product Testing and Test Mark as Proof of*

is quite popular.[118]

Accreditation theorists envision one standard dominating with multiple certifying agents.[119] However, this is unlikely without government intervention. Certification programs will undoubtedly differ as they are initially created, and corporations will choose a program based on subjective factors. The variations will devalue the certifications because the general public will not know what being "certified" means. If one program becomes dominate, corporations will likely gravitate toward it, but the program administrator will be the sole owner of the certification. The monopoly will likely drive certification costs up. The higher costs could leave small and medium-sized businesses unable to afford the certification and could lead customers to forego obtaining services from a certified business for a more cost-effective one.

On the other hand, a government regulation would be free to the public, and certification businesses would have equal access to it. Uncertified corporations would still have to meet the regulation's requirements. Moreover, consumers would have the protections of the regulation regardless of their actions.

Thus, a regulated approach to privacy would offer greater control and protection to consumers. The CCPA offers a balanced approach that grants consumers control of their data while allowing corporations flexibility to develop business strategies around informed or incentivized consent.

B. Trust but Verify: Industry Leadership Versus Government Collaboration

The discussion over data privacy has been controversial, but all agree on the need for data security. The key question has been who is best suited to establish and enforce security measures. Currently, many businesses determine their own security protocols.[120] Proponents of this approach hail this tactic for encouraging security measures that reduce data breaches rather than seizing on opportunities to penalize for such breaches.[121] Further, businesses tend to be more nimble than government and can rapidly adapt to developing technology.[122] Self-regulation,

---

Quality, TÜV RHEINLAND (accessed Sept. 22, 2019), https://www.tuv.com/usa/en/product-certification.html [https://perma.cc/5ET4-ZAQZ]; *A World Leader in Testing, Inspection & Certification Services*, BUREAU VERITAS NORTH AMERICA (accessed Sept. 22, 2019), http://www.us.bureauveritas.com/ [https://perma.cc/3SUD-ESFJ].

118. Two such programs based in the U.S. are administered by the International Association of Privacy Professionals and the Identity Management Institute, respectively. *IAPP Certification Programs*, International Association of Privacy Professionals (accessed Sept. 22, 2019), https://iapp.org/certify/programs/ [https://perma.cc/E45U-CQ5V]; *Certification*, Identity Management Institute (accessed Sept. 22, 2019), https://www.identitymanagementinstitute.org/certification/ [https://perma.cc/Q9T5-L29T].

119. Yuen, *supra* note 69, at 78.

120. *Bottoms Up*, *supra* note 23, at 219 (describing the "bottom up" generally as a voluntary, business-led approach).

121. Mann, *supra* note 21, at 387.

122. Hirsch, *supra* note 57, at 1042.

it is said, promotes innovation.[123] Moreover, proponents argue that public and business goals align as it relates to cybersecurity, and thus, self-regulation is sufficient.[124] Under this approach, data privacy, beyond security measures, would primarily be handled through company-issued contracts with vendors, published privacy practices, and terms of use.[125]

The volume of data breaches,[126] though, is evidence that the corporate sector has fallen short of keeping up with appropriate security measures.[127] The hope had been that through self-regulation, best practices for data protection would be "identified and spread organically" and a "norm" would emerge over time.[128] That thinking is idealistic because, although there may be some synergies, the interests of corporations and consumers in privacy can diverge creating a conflict of interest when businesses have primary responsibility for developing the "rules."[129] Further, allowing internal corporate policies to serve as the entrance to commerce will result in an imbalance in bargaining power between the corporation and the consumer who has little or no opportunity to negotiate changes to the policy.[130] Also, the private nature of internal policies could make whistleblowers the primary source for identifying legally enforceable violations. This reliance would further reduce the power of consumers. Thus, caution must be exercised when applying industry-led laws to public goals like privacy protections.[131]

Recognition of these issues has shaped the development of U.S. cybersecurity laws. The current cybersecurity model is polycentric, meaning that it is "multi-level, multi-purpose, multifunctional, and multi-sectoral."[132] Data security protocols vary by industry sector and are instituted by both industry and government.[133] Sectoral laws tend to be flexible by addressing issues in each industry without overreaching in areas where those regulations are not applicable.[134] The sectoral approach also provides opportunities to experiment with regulatory options and draft solutions unique to the circumstances.[135] Industry-government partnerships should allow the business sector to develop metrics it believes are reasonable and the government to provide oversight.[136] The

---

123. Mann, *supra* note 21.

124. *Id.* at 385 (identifying data security as both a business and consumer interest).

125. Yuen, *supra* note 69, at 65; *see also* Wood, *supra* note 24, at 106.

126. Clement, *supra* note 1.

127. *When Toasters Attack*, *supra* note 29, at 463.

128. *Id.* at 437-38.

129. Hirsch, *supra* note 57, at 1037-38; *see also* Fairclough, *supra* note 24, at 464.

130. Wood, *supra* note 24, at 106.

131. Hirsch, *supra* note 57, at 1042.

132. *When Toasters Attack*, *supra* note 29, at 419 (summarizing the definition of polycentricity).

133. *Id.* at 419-20.

134. Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 873-74 (2009).

135. *Id.* at 873.

136. *When Toasters Attack*, *supra* note 29, at 419-20.

National Institute of Standards and Technology[137] Framework is an example of such a collaboration.[138]

Still, there is room for improvement. The sectoral approach leaves both known and unintended gaps in data protection. Known gaps in data protection are left because, for example, Company C may be subject to Regulation R, but Vendor V, a vendor of Company C, may not.[139] Thus, Patron P's data may be treated securely when it is given to Company C, but less securely when it is shared with Vendor V. Companies have sought to address these gaps through self-regulation and inserting restrictive terms in contracts with their vendors and subcontractors.[140] A federal law mandating a common standard, though, could provide a level playing field for compliance from all businesses without the possibility of such standards being negotiated out of a contract.[141]

Critics also cite the unintended gaps left in data protection when laws are crafted narrowly leaving applicability to new technologies up to judicial discretion.[142] Furthermore, FTC enforcement of "unfair or deceptive" trade practices can have inconsistent results due to broadly written or vaguely stated corporate policies.[143]

One deregulated solution proposes filling the gaps in data protection by forming collaborative working groups of consumers that can monitor various aspects of online activity.[144] Each group would be educated on a particular aspect of data protection, and the interplay between different groups would have to be considered.[145] Consumer advocacy groups can be well-informed and well-organized and have a role to play in protecting the interests of consumers. Still, it seems impractical that such groups would be so prevalent and well-funded as to be able to eliminate the role of government on an issue like data protection that impacts all U.S. residents and has national security and interstate commerce implications. In considering an approach that balances the needs of all stakeholders, consumer advocacy groups might, instead, be most effective in calling attention to data protection issues, prompting the government to act, and representing consumer interests in any collaborative effort to develop new laws.

Polycentric enthusiasts desire flexibility and adaptability,[146] but those

---

137. *Id*. at 441-43; *supra* Section III.C (discussing the NIST Framework and its application in cybersecurity).

138. Id. at 441.

139. Yuen, *supra* note 69, at 45.

140. Wood, *supra* note 24, at 71.

141. Hirsch, *supra* note 57, at 1040.

142. Bellia, *supra* note 134, at 874-75 (discussing the ambiguity in whether YouTube and TiVo are covered by the Video Privacy Protection Act of 1988 which is applicable to "prerecorded video cassette tapes or similar audio-visual materials").

143. Evans, *supra* note 14, at 188; *see also supra* Section III.A (discussing Federal Trade Commission enforcement efforts); Fairclough, *supra* note 24, at 464.

144. *When Toasters Attack*, *supra* note 29, at 438-39.

145. *Id.* at 439.

146. *Id.* at 434.

aspirations can and should be weighed against the interests of consumers. Under the industry-led approach, cybersecurity is seen as *the* way to protect consumer data.[147] Backers of sector-based laws say a broadly applicable baseline law would not address differences in various industries.[148] However, a more regulated or hierarchical approach does not require leaving businesses out altogether. The government still looks, and should continue to look, to industry for guidance on appropriate regulation.[149] "The demand for a more comprehensive legal framework . . . stems from the importance of protecting consumers while facilitating consumer confidence."[150] Focusing on cybersecurity without addressing data privacy leaves out a key component of data security and fails to fill the gaps in data security. Thus, a collaborative approach to cybersecurity that incorporates the expertise of industry, the authority of government, and the needs of consumers provides the best opportunity to protect personal data without hindering commerce.

C. Incentivizing Good Faith: Expanded Liability Versus Statutory Compliance

Collaboration can lead to the dissemination of best practices, but success in preventing the number and impact of data breaches will still primarily rely on business-by-business investment in cybersecurity and compliance with regulations.

The GDPR attempts to incentivize the decision to "invest and comply" by assessing fines of up to four percent of a company's gross revenue.[151] Fines under a similar Brazilian law range up to two percent of revenue.[152] Although some businesses see fines because they are punitive, it is a form of enforcement that can spur businesses to invest in the fast-changing pace of cybersecurity.[153]

Consumer advocates in the U.S., though, want a private right of action.[154] The Federal Trade Commission Act, which gives the FTC primary authority for

---

147. *Id.* at 440.

148. Mann, *supra* note 21, at 386.

149. Hirsch, *supra* note 57, at 1041.

150. *When Toasters Attack*, *supra* note 29, at 440.

151. Reg. 2016/679, *supra* note 38.

152. Melanie Ramey, *Brazil's New General Data Privacy Law Follows GDPR Provisions*, COVINGTON & BURLING LLP (Aug. 20, 2018), https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/ [http://perma.cc/GV4J-FPJA].

153. Patricia Cave, Comment, *Giving Consumers A Leg To Stand On: Finding Plaintiffs A Legislative Solution To The Barrier From Federal Courts In Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 791-93 (2013) (discussing need for monetary penalties as a means of encouraging compliance but capping consumer recovery awards for data breaches where identity theft does not occur).

154. Bellia, *supra* note 134 (discussing Congressional authority to create statutory standing where the courts have found no standing); *see also* Fairclough, *supra* note 24, at 465-66 (discussing the lack of a Constitutional right to privacy in the U.S.).

enforcement of data breach legislation,[155] precludes a private right of action for consumer victims of data breaches.[156] Yet consumers cannot compel the FTC to act on their behalf.[157] The FTC has, instead, called on Congress to create civil penalties against corporations that fail to take reasonable cybersecurity measures.[158] Unlike the GDPR and Brazilian penalties, FTC penalties have been criticized for being too low to be effective.

The California Consumer Privacy Act of 2018 establishes a private right of action for consumers.[159] The insistence on a private right of action is important because tort laws under common law have not adequately protected consumers.[160] Too, courts have both deemphasized the "duty of care" in the digital space[161] and have been reluctant to find harm from data collection and breaches that do not lead to identity theft.[162]

Some corporations argue that a private right of action is unnecessary because consumers accept the risk of cyber hacks by choosing to use the corporation's services.[163] Consumer advocates dismiss the use of Privacy Policies and Terms of Service to elicit consumer consent and call these documents "contracts of adhesion" because consumers have no negotiating power in accepting them.[164] Similarly, consumer assumption of risk, contributory negligence, and license as a means of transferring cybersecurity risks to consumers are not reasonable because the negotiating platform between consumers and corporations is not level.[165] Moreover, because corporations traditionally withhold detailed information about the extent of collection and use of consumer data, the average customer is unable to understand, assume, or control the risk.[166]

Thus, it is essential to advance legal parity between businesses and consumers by enacting a private right of action and legal acknowledgment of an individual's right to own their data.

Others believe a company's duty of care to protect customers from harm

---

155. *Supra* Section III.A (explain the FTC's role in data protection enforcement).

156. Mann, *supra* note 21, at 385.

157. *Id.*

158. *Id.*

159. 1.81.5 CAL. CIV. CODE § 1798.100 (2019).

160. Fairclough, *supra* note 24, at 465-66 (stating that Americans do not own their personal data and discussing the lack of a Constitutional right to privacy in the U.S.).

161. Wood, *supra* note 24, at 109-11 (discussing the duty of care in tort law and the Court's lack of emphasis on the duty in civil actions).

162. Fairclough, *supra* note 24, at 466, 471 (discussing the judicial finding that an advertiser's use of personal information did not deprive the consumer of a monetary harm); *see also* Cave, *supra* note 153, at 768-69, 776, 778-79.

163. Wood, *supra* note 24, at 106 (discussing the contract law argument for consumer consent and the lack of consumer negotiating power).

164. *Id.* at 86. (discussing the contract law argument for consumer consent and the lack of consumer negotiating power).

165. *Id.* 103-06.

166. *Id.*

should extend to the corporate officers who make decisions. In their roles as corporate leaders, business executives are stewards of the public trust as it relates to data protection.[167] Although corporations can be held liable for breaches, executives are shielded through business laws such as agency protections and the business judgment rule.[168] When a corporation is held liable for breaches, the penalties are paid, albeit indirectly, by shareholders who have little control over corporate governance or are redistributed to suppliers and customers instead of being borne by corporate leaders.[169]Advocates for holding executives personally liable for data breaches argue that civil and criminal liability for decisions they make will refocus attention on data protection and reduce excessive risks taken with consumer data.[170]

Implicating executives personally, when no malicious or fraudulent behavior has occurred, is flawed in many regards. First, the protections of incorporation are lost under this approach. Changing veil-piercing and agency laws and stripping executives of these defenses in litigation would take a change to statutory laws across the country at state and federal levels and change international trade.[171] This approach minimizes the complexity of this action.

Holding executives personally liable for nonfraudulent acts makes business ownership an even riskier proposition than it already is. Too, that approach is likely to stifle innovation, entrepreneurship, and leadership because the best leaders may be disincentivized to step into corporate leadership. Less effective leadership can harm a corporation, and perhaps the overall economy, in the long-term.

Invalidating corporate laws will not stop indemnity clauses in employment contracts from protecting executives. Executives could still be protected, but agency laws would be weakened, making it more difficult for consumers to recover from the corporation directly.

Finally, the executive liability approach proposes that executives should be acting in the best interest of the public. If executives must act in the best interest of the public, then no one is left to act on behalf of the corporation and its interests. This approach ignores this inherent conflict of interest. Instead, to address corporate dominance in developing legislative and social policy, government actors and consumer activists should serve as a counterbalance to executives necessarily acting in the interest of corporations.

---

167. *Id.* at 66.

168. *Id.* at 67, 97 (noting that the business judgment rule generally says executives are not liable for decisions they make on behalf of the corporation if the decision is made in good faith and with the interest of the corporation in mind).

169. *Id.* at 100-01.

170. *Id.* at 65-71 (explaining that data breaches are the result of lack of investment in cybersecurity, that executive compensation discourages investment in cybersecurity, and that civil and criminal liability for executives will incentivize the necessary investment).

171. *See generally id*. (generally arguing for changes to agency law and the business judgment rule and reduction of affirmative defenses like assumption of risk, contributory negligence, and license).

Instituting civil fines for data breaches, establishing a private right of action, and expanding the liability of corporate executives all incentivize "investment and compliance" by punitive means after a breach has occurred. Ohio has taken a different approach by limiting liability for businesses that show an upfront investment in cybersecurity: The Ohio Data Protection Act ("Ohio law") was enacted in 2018.[172] The law lists eight industry or federal statutory security frameworks, including the NIST Framework, GLBA, and HIPAA,[173] that a business can implement to be covered by the law.[174] It protects Ohio businesses from litigation after a data breach by allowing the pre-breach implementation of one of the listed frameworks to serve as an affirmative defense to tort liability claims.[175] Breaches due to third-party data sharing are not protected, and existing breach notification laws are not affected by the law.[176]

Drafters of the Ohio law hope that companies will invest in one of the frameworks to receive the protections of the law, thus reducing the chances of suffering a breach and leading to greater protections for consumer data.[177] The law has weaknesses, however. Some of the security frameworks are existing federal laws that already require compliance.[178] Further, many established, large-scale, or high cyber-risk businesses have already incorporated the cybersecurity standards identified within the Ohio law.[179] In both cases, the law offers additional protections with no additional effort on the business' part.

Moreover, giving the protection of an affirmative defense may disincentivize corporations from doing more than these minimum standards to protect consumer data. Prior to implementation of the Ohio law, corporations could still use implementation of cybersecurity standards to defend against tort claims, but the defense was not affirmative.[180] Thus, a corporation might have to prove a reasonable standard of care as it relates to data protection overall, not just data

---

172. Provide Legal Safe Harbor if Implement Cybersecurity Program, S.B. 220, 132d Gen. Assemb. (Ohio 2018); *see also* Scot Ganow & Zachary Heck, *Proactive Approach to Cybersecurity Pays off in Ohio with New Data Protection Act*, LEXOLOGY (Aug. 13, 2018), https://www.lexology.com/library/detail.aspx?g=d5e245e4-f2b5-4665-9e95-bf1973c875ac [https://perma.cc/J3WC-S2U3].

173. S.B. 220, 132d Gen. Assemb., Reg. Sess. (Ohio 2018). The acronyms stand for National Institutes for Science and Technology, Gramm-Leach-Bliley Act, and Health Insurance Portability and Accountability Act. *See generally* Section III (discussing NIST, GLBA, and HIPAA).

174. Ganow & Heck, *supra* note 172.

175. *Id.*

176. *Id.*

177. *Id.*

178. S.B. 220, 132d Gen. Assemb. (Ohio 2018) (The Ohio Law provides an affirmative defense from liability to organizations that comply with GLBA, HIPAA, the Federal Information Security Modernization Act of 2014, and the Health Information Technology for Economic and Clinical Health Act, which are all federal laws to which compliance is already required.).

179. Corley, *supra* note 37, at 743-44 (discussing corporate cybersecurity efforts including encryption tools and creation of Do-Not-Track technology).

180. *See* Ganow & Heck, *supra* note 172.

security.

This difficulty creates a legal imbalance against consumers and in favor of businesses that already tend to have greater control and resources in litigation. Consumer victims of corporate data breaches would not have any means of redress upon the corporation showing that one of the security frameworks was in place before the breach. Thus, while the Ohio law can be useful for establishing minimum security standards in all industries, allowing those standards to serve as an affirmative defense against consumer liability claims does not balance the interests and legal rights of consumers.

D. Applicability to All: Data Protection for Small Businesses

The privacy provisions of both the GDPR and CCPA have exclusions for smaller businesses in recognition of the reduced risk and greater cost of compliance. While it is reasonable to account for the higher burden regulations place on smaller firms, all businesses bear responsibility in their business practices. A company that is willing to invest in the technology for data mining, for instance, should not then say they have no money to protect that data. The burden of securing personal data is lessened by not collecting unnecessary data and deleting data that is no longer needed. Thus, application of the CCPA privacy provisions to smaller companies could drive good business practices and minimize cybersecurity costs.

While data privacy can be more process-driven, data security is often a continual process of outwitting would-be hackers. Best practices such as retaining a privacy officer on staff, weekly or even daily system tests, and frequent technology upgrades may not be feasible for the size and revenue of the business. Furthermore, depending on the type of business, such measures may not be necessary. These realizations should not completely absolve a small business from liability. Still, to ensure entrepreneurship is not suffocated by costly regulations, a "practical steps" standard should be applied to low-risk, small-volume businesses. Practical steps would include data encryption, password protection, firewall software, and similar measures.

In terms of breach response requirements, there may not be an easy answer for small businesses. The widespread use of email addresses and the smaller volume of customers should help make notification via email affordable. Having a single preemptive federal law would lessen the cost and burden of having to understand and comply with fifty state breach notification laws.

Small businesses warrant special consideration in determining penalties for violations of data protection laws, whether a law is state or federal. Whereas a private right of action could incentivize large corporations to spend the money to institute better practices, high litigation costs could force bankruptcy and dissolution of a small company. Still, consumers should have some protections against negligent or willful disregard of data protection laws. Thus, civil fines issued by a government agency are a good option to strike the right balance between protecting consumers and promoting entrepreneurship. Such fines should be tiered based on factors to include the effort made by the small business to avoid a violation, the harm caused by the violation, and the number of violations.

It is worth noting that cyber insurance is a good way to mitigate financial damages due to a data breach.

For companies in general, but small businesses in particular, the simplicity of a single preemptive federal law would make compliance with data protection regulations more feasible, both economically and logistically, over adherence to a multitude of state laws. The continuous proliferation of hundreds of state regulations is burdensome and costly to monitor, understand, and adjust operations for. This is true as it relates to privacy protections, cybersecurity, and breach notification. High-risk small businesses in critical sectors like healthcare and banking would still be regulated by applicable federal sector laws.

VI. PROPOSAL FOR A COMPREHENSIVE FEDERAL DATA PROTECTION LAW

The proposal of this Note for a comprehensive federal data protection law is an attempt to (1) improve data security to minimize harm from cyber attacks, (2) reduce the challenges and costs businesses face in complying with so many different laws, (3) recognize and balance the rights of consumers, and (4) achieve these goals while remaining true to the American virtues of exercising the democratic process and supporting entrepreneurship and innovation.

A. Improving Data Security

The technological nature of our society will continue to necessitate a heavy focus on cybersecurity in all data protection efforts. All businesses should be required to maintain adequate data security as an implied warranty to its customers when the data is collected and as affirmative compliance with data protection laws.

What is "adequate," however, may vary by the nature and size of the business. Establishing a security metric for all businesses based on what is reasonable for Target, Equifax, or Facebook, for instance, may cripple small businesses and hinder the entrepreneurial spirit that has been key to American innovation and economic success. Thus, the sectoral method for addressing data security is practical.[181] This method, though, should be enhanced by legally enforceable minimum cybersecurity standards that can be implemented by all businesses.

In this regard, the Ohio law's effort to define minimum security metrics for businesses can be an effective part of a comprehensive solution to data protection.[182] Meeting such minimums, however, should not be a pass for organizations not to do more. Nor should they be an escape from liability for consumer harm when there is a data breach. An affirmative defense to liability, as is included in the Ohio law, can leave consumers without redress for security breaches they have no power to prevent. This higher risk could deter some consumers from fully participating in the marketplace. Besides, businesses are

---

181. *See supra* Section V.B (discussing sector-based regulations).

182. *See supra* notes 172-80 and accompanying text (discussing the security provisions of the Ohio Law).

better suited to handle the liability because they control the security measures used and because they are better able to insure against economic risks.

Enforcement is a crucial component of compliance. Government-imposed penalties should be significant enough to incentivize implementing effective cybersecurity systems and complying with regulations. At the same time, consumer legal rights should be supported by the recognition of ownership rights of personal data and enactment of a private right of action.

The business sector should be highly engaged in determining what the minimum-security standards are and what additional measures can help secure specific industries. Consumer advocates and government agencies, on behalf of individuals, must take a stronger role in ensuring standards are high, effective, and enforceable under the law.

B. Ease of Corporate Compliance

Complying with the vast number of data protection laws is a challenge for businesses.[183] Having uniformity among states would aid businesses by creating single-law compliance. The most efficient way to create such uniformity is through preemption of state laws with a federal law. Congress derives its right to preempt state laws from the Commerce Clause of Article I and the Supremacy Clause of Article VI of the Constitution.[184]

Federalism advocates consider the development of a federal law an overreach of power.[185] However, this line of thinking does not place adequate emphasis on the national and global nature of commerce. Even small businesses selling through a website can be subject to regulatory compliance with laws across the country.

Creation of a federal law would also create procedural efficiencies for businesses. In 2010, the U.S. Department of Commerce proposed a Privacy Policy Office to focus on all data protection issues and coordinate with the FTC.[186] Others have called for Congress to delegate explicit authority over data protection enforcement issues to the FTC.[187] The GDPR requires a single office in each country to handle all data protection matters.[188] A federal law administered through one agency would create a single source for interpretation of laws, implementation of standard procedures, and establishment of compliance processes. The FTC is the most logical agency to accept this role, given its current involvement with data protection laws.[189]

Another benefit of a comprehensive federal law is greater confidence in

---

183. *See supra* Section III.B (discussing the vast number of state laws).

184. Cave, *supra* note 153, at 789.

185. Bellia, *supra* note 134, at 870 (summarizing anti-Federalization arguments as discussed in Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902 (2009)).

186. Mann, *supra* note 21, at 389.

187. *Id.* at 388.

188. Regulation (EU) 2016/679, *supra* note 38.

189. *See supra* Section III.A (discussing the FTC's role in data protection and enforcement).

American businesses by an international community that is increasingly focused on consumer privacy and is looking for a means of enforcement of their laws against U.S. businesses.[190]

C. Recognition of Consumer Rights

A consistent theme in the many approaches for improving data protection is the differing interests of businesses and consumers. There is a need to "balance business goals (i.e., profit-seeking and efficiency) with increasingly vocal consumer concerns over data privacy."[191] A necessity in striking this balance is for the business sector and government to recognize that data privacy is a means of data security. Addressing data privacy is a "*proactive* means of preempting the breach and misuse of transferred information."[192] Further, businesses should not assume or fear that consumer control over personal data will mean that consumers will not willingly share data. To the contrary, the popularity of Google Home®, Amazon's Alexa®, and other such devices arguably prove otherwise. Instead, giving consumers this control can help companies more easily identify their target customers while still displaying a "consumer-concerned" brand.

Data privacy laws provide a baseline for data security that all businesses can meet. The privacy provisions of the CCPA should be adapted into federal data protection legislation.[193] Companies have made opting out difficult by not providing prior notice of this option, burying the option in fine print or complicated documents, and in some cases requiring customers to mail in their selection. Further, many websites start collecting data as soon as they load rather than waiting for the consumer to opt-out. Moreover, on many websites opting out does not include opting out of data collection by the websites' third-party vendors; thus, the consumer really hasn't been afforded the opportunity to opt out. Therefore, the opt-in provisions of the GDPR would be more effective in ensuring consumers are genuinely able to exercise the choice to opt out of data collection.[194] Alternatively, opt-out notifications should be obvious, genuine, offered before collecting the data, and easy for customers to select.

In addition to controlling access to their data, consumers need the legal right to obtain redress for misuse of their data. The consumer's private right of action is consistent with the historical American ideal of the "right to be let alone," with the concept of implied warranties in contract law, and with the development of "duty of care" in tort law.[195] Laws that hamper an individual's use of the judicial

---

190. *See supra* notes 36-42 and accompanying text (discussing the E.U.'s lack of confidence in U.S. laws and direct evaluation of businesses by the E.U. for data protection compliance).

191. Yuen, *supra* note 69, at 3.

192. *Id.* at 38.

193. *See generally supra* Section V.A. *See also supra* notes 105-10 and accompanying text (discussing the privacy provisions of the CCPA).

194. *See supra* note 111 and accompanying text (discussing opt-out versus opt-in provisions).

195. *See supra* Section III (discussing the history of privacy); *see also supra* notes 155-66 and accompanying text (discussing the private right of action).

system in remedying harm create an unfair advantage for businesses which often have a financial advantage already.[196] Such laws can also disincentivize corporations from taking the greatest measures feasible to protect data both as a privacy matter and a security measure.

While laws that include a per-person fine for violations incentivize organizations to focus on compliance and maintain the highest security measures practicable, they are punitive and not associated with the harm caused to consumers.[197] Part of the balancing act necessary to create a comprehensive federal law must be an acknowledgment that the "true criminals" are hackers, not businesses, and hackers are constantly targeting businesses. When a business has (1) taken appropriate steps to protect data privacy, (2) committed adequate resources to data security, and (3) complied with cyber laws, assessing punitive penalties is not appropriate. However, when companies fail to take such measures, higher fines of up to four percent, as called for under the GDPR, are proper.

D. Maintaining American Norms

It is essential to the growth of American commerce to protect against cyber hacking, maximize opportunities for international trade, ease regulatory compliance, and balance consumer privacy rights. However, these things must be done in a way that does not jeopardize the American economy or investment in innovation and in a manner that respects the American legal system and societal norms. This proposal seeks to balance these interests by maintaining business' engagement in the development of legislation; by minimizing disruption of current laws and long-standing customs of commercial trade;[198] and by recognizing sector-specific issues while modernizing historical privacy rights and reinforcing individual access to the judicial system.

Sustaining an entrepreneurial culture is imperative.[199] A federal law will ease compliance over the management of multiple state laws.[200] Further, data protection laws can be crafted to allow existing small businesses to take "practical steps" to improve cybersecurity, minimize litigation costs for small businesses, and give them time to phase-in any new requirements.[201]

---

196. *See supra* note 180 and accompanying text (arguing against the Ohio laws that provide corporations with an affirmative defense to liability).

197. *See supra* notes 151-58 and accompanying text (discussing penalties as a means regulatory enforcement).

198. *See supra* notes 167-71 and accompanying text (arguing against data protection approaches that change veil-piercing and agency laws).

199. *See supra* Section V.D (discussing the applicability of data protection to small businesses).

200. *See supra* notes 71-73 and accompanying text (explaining that state laws require businesses to comply with hundreds of different data protection laws).

201. *See supra* Section V.D (discussing the applicability of data protection to small businesses).

A final consideration is that of national security. Comprehensive federal data protection can plug state law security gaps, thus serving national security interests by helping to reduce the number and impact of data breaches.

VII. CONCLUSION/ RECOMMENDATION

All three branches of the federal government are grappling with how to address control of privacy rights and liability for data breaches.[202] The CCPA has spawned the passage of a rash of state privacy laws over the past year and will serve as the tipping point for the implementation of a federal data privacy law. States will continue to promulgate differing laws until the cost and frustration of corporate compliance forces action at a national level.[203] This frustration is already evident with more of the business sector calling for a federal law.[204]

The effort put into crafting a federal law should not, however, just focus on privacy. Federal regulations should recognize individual privacy rights, enact minimum cybersecurity standards, simplify security breach response, and increase efficiency in compliance and enforcement of cyber laws. Thus, this proposal urges passage of a preemptive federal data protection law that includes:

(1) adaption of the CCPA privacy provisions to include opt-in provisions,[205]
(2) minimum cybersecurity standards for businesses based on risk and industry type,
(3) continuation of heightened cybersecurity measures for large corporations and high-risk industries,
(4) structured expansion of data protection provisions to include small businesses,
(5) one standard breach response procedure,
(6) civil penalties for negligent or willful violations of data protection laws of up to four percent of company revenue.
(7) individual privacy rights and a private right of action, and
(8) establishment of a single authority (likely the FTC) for data protection law enforcement.

Passage of this legislation will properly balance individual privacy rights with continued strides in corporate innovation.

---

202. *See supra* Sections III.A-B (discussing the current status of U.S. data protection laws).

203. Forbes Technology Council, *supra* note 72 (predicting that many states will be adding and changing their privacy laws).

204. *See supra* Section IV (discussing the momentum towards a federal data protection law).

205. *See generally supra* note 111 and accompanying text (describing opt-out provisions that would also be acceptable).