"IF YOU WANNA STEAL MY DATA YOU GOTTA BE A U.S. BASED CORPORATION!"[1]: INEFFICIENCIES ABOUND IN THE ABSENCE OF FEDERAL DATA PROTECTION REGULATIONS

By: Hillary Healey[*]

I. INTRODUCTION

What are data protection regulations? Why should companies and consumers care about them?

The U.S. is behind the rest of the world when it comes to instituting broad data protection legislation. U.S. companies may be spending more than necessary to comply with varying global and anticipated state

* The author is a graduate of the University of Houston Law Center, class of 2022, and is a *Houston Business & Tax Law Journal* alumnus. The author is currently an associate attorney in the corporate group at Akin Gump Strauss Hauer & Feld LLP. She would like to thank the *Houston Business & Tax Law Journal* editorial team for their help and guidance in writing this article.

1. @weems, TWITTER (Aug. 1, 2020, 12:48 AM), https://twitter.com/weems/status/1289437744997924867?s=20.

legislation. This problem is exacerbated when considering whether companies are complying in the first place, and if there is any evidence this cost is passed on to the consumer. Omnibus federal regulations could potentially save businesses money. Varying regulations put an increased risk on corporations and a greater burden on consumers. This all begs the question: what does compliance currently look like? This note explores how data protection compliance could be made more economically efficient for U.S. businesses while granting consumers appropriate protection and avoiding impractical and costly over-regulation.

The current data privacy landscape provides more questions than answers. Personal data is a hotter commodity than ever, and unauthorized access to this information is one of the most powerful weapons of the twenty-first century. This data is valuable for businesses, enabling a technological revolution in buying and selling. Consumers also benefit from the corporate aggregation of their personal data, which is apparent in the ever-increasing ease of access to marketplaces across industries. Constant, research-based innovations would be impossible without such information. Corporations currently use personal data aggregation in marketing and advertising campaigns to target and tailor ads to assist shoppers rather than pestering them with irrelevant advertisements. However, the risks that accompany the collection and storage of personal data put these novel opportunities at jeopardy. This risk is reflected in every data breach and site hack, bringing the U.S. lack of national data protection strategy into the limelight.

Currently, "[t]he United States does not have a national law that prescribes specific data security standards for all industries."[2] U.S.-based corporations with an online presence must navigate a global hodgepodge of regulations, including South American law[3], the E.U.'s General Data Protection Regulation (GDPR)[4], the California Consumer Privacy Act (CCPA)[5], the Health Insurance Portability and Accountability

2. Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2213 (2019) (quoting Jeff Kosseff, CYBERSECURITY LAW 1 (2017)).

3. *See generally* CYNTHIA RICH, BL BUREAU NAT'L AFFS., PRIVACY IN LATIN AMERICA AND THE CARIBBEAN 1 (2015) (providing an overview of South American internet regulations).

4. Regulation 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, 2016 O.J. (L 119) 87.

5. CAL. CIV. CODE § 1798.100 (West 2021).

Act (HIPAA)[6], the Gramm-Leach-Bliley Act (GLBA)[7], and various state laws.[8]

Compliance with such a complicated global framework makes risk mitigation a near-impossible task.[9] It is also an exorbitantly expensive one. Some critics believe proper compliance is not even within the market's current capability, calling for national regulations that would offset compliance costs for U.S. corporations.[10] This note will explore a future where federal omnibus legislation creates economic efficiencies and argues that the benefits of centralized regulation, enforced through existing agency frameworks, is the best solution to protect consumers.

Part II of this Comment explains the current legislative landscape regarding data privacy on both the state and federal levels. This section also explores the current costs of compliance. Part III confronts a common problem for many U.S. corporations: the current disjunctive web of laws and regulations, while offering possible federal solutions. Part IV will explore how exactly such solutions can be effectively enforced.

AUTHOR'S NOTE: This article was submitted for publication in 2020 prior to the presidential election and change in administration.

II. WHAT DOES DATA PRIVACY LAW AND COMPLIANCE LOOK LIKE RIGHT NOW?

A. State Legislative Landscape

State consumer privacy law is sparse in much of the country, but a few states have begun enacting limited legislation.[11] This area of law seemed to be evolving rapidly at the state level prior to the COVID-19 pandemic.[12] Although focus shifted away from consumer privacy legislation for much of 2020, the inauguration of President Joe Biden is

---

6. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 221, 110 Stat. 1936 (codified as amended at 42 U.S.C.A § 1320a-7); *see also* Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5, § 123 Stat. 226 (2009) (amending and expanding certain HIPAA privacy protections).

7. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 132, 113 Stat. 1338 (1999).

8. *See* Wendell J. Bartnick, *Present and Future Data Privacy Outlook*, 24 CURRENTS: J. INT'L ECON. L. 70 (2020).

9. *Id.*

10. John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 468 (2018).

11. *2020 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES, (Jan. 17 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.

12. Xavier Clark & Nyika Corbett, United States: Countdown To 2021: Privacy & Data Security, Mondaq (Dec 23 2020), https://www.mondaq.com/unitedstates/data-protection/1019494/countdown-to-2021-privacy-data-security.

expected to catapult this issue back into the spotlight, both on the state and federal level.[13]

Currently, California is the most progressive state when it comes to consumer privacy, leading the charge in this area.[14] The state of California passed the CCPA in 2018, which became effective as of January 1, 2020.[15] The Act gives California citizens broad rights to disclosure, access, and deletion of much of their personally identifiable information, mirroring the E.U.'s notice-and-consent model implemented by the passage of GDPR earlier in 2018.[16] The state of California have continued to take even stronger action, passing Proposition 24 on November 3, 2020, which approved the California Privacy Rights and Enforcement Act (CPRA).[17] The CPRA appears to be a referendum on legislative and big tech opposition to the CCPA, affirming the citizenry's desire to expand and strengthen the protections granted by the CCPA.[18] CPRA strengthens regulations with new requirements for corporations that collect and share personal information.[19] It also creates the California Privacy Protection Agency, an entirely new enforcement agency responsible for CPRA violations.[20]

Massachusetts is another state that has been an early adopter of European-style consumer privacy and data security laws.[21] The Massachusetts Data Security Regulation legislation includes some of the

---

13. Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS: TECH TANK (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ ("Democratic nominee Joe Biden is on the record supporting comprehensive privacy legislation. Thus, a Biden administration would likely play a role in privacy regardless of which party holds the Senate.").

14. *See, e.g.,* The California Privacy Rights Act of 2020, CA Prop. 24 (2020), 2020 Cal. Legis. Serv. Prop. 24 (WEST) ("Rather than diluting privacy rights, California should strengthen them over time."); Letter from Xavier Becerra, State of California Attorney General, to Congress on CCPA preemption (Feb. 25, 2020), https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20on%20CCPA%20preemption.pdf (inviting congress to look to the states as a source of innovation in data privacy and urging Congress not to preempt the CCPA with federal legislation).

15. CAL. CIV. CODE § 1798.100 (West 2021) (Added by Stats. 2018, c. 55 (A.B.375), § 3, eff. Jan. 1, 2019, operative Jan. 1, 2020.).

16. See Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, Practical Law Practice Note Overview W-016-7418, THOMPSON REUTERS (database updated 2020).

17. *Id.*

18. See *Californians For Consumer Privacy Submits Signatures to Qualify the California Privacy Rights Act for November 2020 Ballot*, CALIFORNIANS FOR CONSUMER PRIVACY (May 4, 2020), https://www.caprivacy.org/californians-for-consumer-privacy-submits-signatures-to-qualify-the-california-privacy-rights-act-for-november-2020-ballot/ (explaining that Prop. 24 qualified for the November 2020 ballot with over 900,000 signatures).

19. *See* CAL. CIV. CODE tit. 1.18.5, §§ 1798.100 et seq. (West 2021).

20. Paul W. Sweeny, Tara C. Clancy, and Gregory T. Lewis, *California Voters Approve (Another) Overhaul of California Consumer Privacy Laws: Meet the California Privacy Rights Act,* NAT'L L. REV. (Jan. 13, 2021), https://www.natlawreview.com/article/california-voters-approve-another-overhaul-california-consumer-privacy-laws-meet.

21. *See* 201 MASS. CODE REGS. §§ 17.01-17.05 (The Massachusetts Data Security Regulation has a compliance deadline of March 1, 2020).

most comprehensive state-level data security regulations in the U.S.[22] Like the CCPA, these regulations apply to any business that touches data of Massachusetts residents, regardless of whether the business is located in Massachusetts.[23] The Massachusetts law provides further protection by using strict security program requirements that are missing from the CCPA.[24] In comparison, the CCPA focuses on establishing certain private rights of action for citizens when data breaches occur as a result of a lapse in security procedures.[25]

Maine and Nevada also have internet privacy laws offering varying degrees of protection for consumers. Maine's legislation is notable because it explicitly prohibits the use, sale, disclosure, or permission to access a customer's personal information without opt-in consent, subject to few exceptions.[26] Nevada's Amended Online Privacy Law provides consumers with the right to opt out of the sale of their information by corporations with a virtual or physical presence in the state.[27]

At the beginning of 2020, Virginia, Florida, New Hampshire, Washington, Nebraska, New York, Maryland, and North Dakota were each expected to attempt to pass consumer privacy legislation similar to the CCPA.[28] The COVID-19 pandemic delayed many of these efforts until at least 2021.[29]

On the other hand, some states, such as Massachusetts, continued to make legislative progress throughout the pandemic.[30] In August 2020, Massachusetts established a Data Privacy and Security Division, tasked with enforcing the state's Consumer Protection Act and the data breach notification law.[31] Additionally, Vermont's Security Breach Notice Act was amended and took effect July 1, 2020 expanding the definitions of personally identifiable information and data breaches to

---

22. *Id.*

23. *Id.*

24. *Id.*

25. *Compare* Jehl & Friel, *supra* note 16, *with* 201 MASS. CODE REGS. §§ 17.01-17.05 ("The CCPA does not directly impose data security requirements. However, it does establish a private right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk.").

26. ME. STAT. tit. 35-A § 9301 (2020).

27. NEV. REV. STAT. ANN. §§ 603A.340 & 603A.345 (West 2021).

28. Cynthia Brumfield, *Passage Of California Privacy Act Could Spur Similar New Regulations In Other States*, CSO (Nov. 12, 2020), https://www.csoonline.com/article/3596295/passage-of-california-privacy-act-could-spur-similar-new-regulations-in-other-states.html ("Prior to the COVID pandemic, 'Approximately eight other states had a copycat version of the CCPA in the works,' Peter Stockburger, partner in the Data, Privacy and Cybersecurity practice at global law firm Dentons, tells CSO.").

29. *Id.*

30. *See* 201 MASS. CODE REGS. §§ 17.01-17.05 (2021).

31. Adam Salter & Drew Broadfoot, *Jones Day Cybersecurity, Privacy & Data Protection Lawyer Spotlight: Kerianne Tobitsch*, 26 JONES DAY PRIV. & CYBERSEC. UPDATE, *Nov. 2020* (further explaining that although the agency is not tasked with explicit enforcement of consumer privacy, it is a notable step in the right direction).

further protect consumer privacy.[32] On the same date, Vermont's Student Data Privacy law also went into effect, preventing operators from using student's personal information for advertising or sale and providing public notice requirements and a right to deletion for institutions.[33]

Regardless of the impact of the COVID-19 pandemic, consumer privacy legislation in other states has not had as much success when compared with Massachusetts and Vermont. In March 2020, data privacy legislation failed to pass in the Washington state legislature for the second time.[34] It is important to note that setbacks, such as the one in Washington, are likely to reverse course during the next administration.[35] Many states that have yet to take formal legislative action have begun to form advisory bodies to investigate and analyze the consumer privacy landscape. Texas, for example, has failed to advance any consumer privacy legislation thus far. However, the state did form the Texas Privacy Protection Advisory Council in 2019.[36] In September 2020, the council issued interim recommendations on proposed data privacy changes for the state.[37]

B. Federal Legislation on the Horizon

Federal consumer privacy legislation may be on the horizon during the next administration. As recently as September 23, 2020, the Senate Committee on Commerce, Science, and Transportation held a hearing to "examine the current state of consumer data privacy and legislative efforts" to guide data protection.[38] The committee discussed U.S. state

---

32. VT. STAT. ANN. tit. 9, § 2435(b)(2) (West 2020).

33. *Id* at § 2443(e)(5).

34. S.B. 6281, 2020 Leg., 66th Reg. Sess. (Wash. 2020)**;** *See* Jennifer Bryant, *Washington Privacy Act Fails For Second Time*, IAPP (Mar. 13, 2020), https://iapp.org/news/a/washington-privacy-act-fails-for-second-time/ ("A version of the bill that passed through the Senate with a 46-1 vote in February would have granted enforcement authority to the state attorney general.").

35. Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS: TECH TANK (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/.

36. *Governor Abbott Appoints Five To Texas Privacy Protection Advisory Council,* OFF. OF THE TEX. GOVERNOR (Nov. 4, 2019), https://gov.texas.gov/news/post/governor-abbott-appoints-five-to-texas-privacy-protection-advisory-council; H.B. 4390, 86th Leg., Reg. Sess. ¶¶ 1–3 at 1 (Tex. 2019).

37. TEX. PRIV. PROT. ADVISORY COUNCIL, SEPTEMBER 2020 REPORT, 86th Tex. Leg. Sess. at 11-12, https://senate.texas.gov/cmtes/86/c990/c990.InterimReport2020.pdf; *See also* David Stauss, *Texas Privacy Protection Advisory Council Issues Interim Report*, HUSCH BLACKWELL: BYTE BACK (Sept. 13, 2020), https://www.bytebacklaw.com/2020/09/texas-privacy-protection-advisory-council-issues-interim-report/ ("The report provides five recommendations for proposed privacy legislation in Texas but does not propose specific statutory language or make recommendations on many key issues.").

38. Caitlin Wilmot, *Sept. 23rd Senate Committee Hearing on Federal Data Privacy Legislation*, ROTHWELL FIGG: PRIVACY ZONE (Sept. 23, 2020), https://www.jdsupra.com/legalnews/sept-23rd-senate-committee-hearing-on-12385/; *Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the Comm. On* Com., Sci., & Transp., 116th Cong. (2020).

privacy laws, the GDPR, and COVID-19 legislation as possible models for federal consumer privacy law.[39] Although such a hearing seems promising, in reality, a divided Congress will battle over this type of legislation if any bills gain steam in 2021.[40] The question of preemption of state consumer privacy laws is subject to powerful influences, including the Silicon Valley giants that first opposed the CCPA.[41]

Interestingly, a strong call from the public for federal legislation, such as the one seen during the November 2020 election in California, is not a driving force behind efforts to introduce federal preemptive legislation.[42] However, it is possible that it may develop in the future, especially in the wake of the implementation of the CPRA.

The Biden-Harris administration may attempt to bolster support for data privacy legislation by creating a bipartisan coalition.[43] If this particular legislation is pushed through in a bipartisan effort, it would be a significant accomplishment for the administration, especially considering the divisive political climate of early 2021.[44] Since the middle of 2018, representatives from both sides of the aisle have drafted proposals for federal privacy legislation.[45] The Safe Data Act (Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act) was referred to the Senate Committee on Commerce, Science, and Transportation in September 2020.[46] The Republican-sponsored bill was killed on December 31, 2020, in the midst of one of the most contentious political periods in American history.[47] But earlier in 2020, the House Subcommittee responsible for

---

39. Wilmot, *supra* note 38; *Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the Comm. On* Com., Sci., & Transp., 116th Cong. (2020).

40. Kate Kaye, *Cheat Sheet: What To Expect In State And Federal Privacy Regulation In 2021*, DIGIDAY (Feb. 1, 2021), https://digiday.com/media/ cheatsheet-what-to-expect-in-state-and-federal-privacy-regulation-in-2021/ ("For now, there's really no telling whether legislators will come to together on preemption and the right to legal action, or whether they'll remain points of contention blocking federal privacy law.").

41. Cynthia Brumfield, *Passage Of California Privacy Act Could Spur Similar New Regulations In Other States*, CSO (Nov. 12, 2020), (November 12, 2020, 3:00 AM) https://www.csoonline.com/article/3596295/passage-of-california-privacy-act-could-spur-similar-new-regulations-in-other-states.html.

42. *Id.*

43. Lucas Ropek, *Privacy Policy and the Biden Presidency: A Promising Outlook?*, GOV'T TECH. (Dec. 9, 2020), https://www.govtech.com/security/Privacy-Policy-and-the-Biden-Presidency-A-Promising-Outlook.html ("With the incoming Biden administration, the federal government may be well positioned to finally preside over a robust privacy agenda.").

44. Kathryn M. Rattigan, *The Effect of a Biden-Harris Presidency on Privacy in the U.S.*, NAT'L L. REV. (Nov. 12, 2020), https://www.natlawreview.com/article/effect-biden-harris-presidency-privacy-us.

45. *Id.*; Gregory M. Kratofil, Jr. & Elizabeth Harding, *Federal Privacy Legislation Update: Consumer Data Privacy and Security Act of 2020,* NAT'L L. REV. (March 14, 2020), https://www.natlawreview.com/article/federal-privacy-legislation-update-consumer-data-privacy-and-security-act-2020.

46. Safe Data Act, S. 4626, 116th Cong. (2020); Müge Fazlioglu, *Consolidating US Privacy Legislation: Safe Data Act*, IAPP: PRIVACY TRACKER (Sept. 21, 2020), https://iapp.org/news/a/consolidating-u-s-privacy-legislation-the-safe-data-act/.

47. Safe Data Act, S. 4626, 116th Cong. (2020).

drafting federal privacy legislation, the House Energy and Commerce committee's subcommittee on Consumer Protection and Commerce, worked through the pandemic to stress the need for bipartisan support of a bill for national data privacy standards.[48] The new administration would likely not only encourage more movement in Congress, but may also even see the Federal Trade Commission (F.T.C.) adopt heightened scrutiny or a more active enforcement scheme.[49]

Currently, three main policy issues prevent a bipartisan effort on federal consumer privacy legislation. The first divisive issue is how to enforce a requirement that companies notify the appropriate authorities whenever a data breach occurs.[50] The second issue is that Congress must agree on whether or not federal legislation should preempt current state laws, either completely or partially.[51] Lastly, the representatives remain divided over whether consumers should have the private right to bring class-action suits against corporations that violate any new federal standards.[52]

C. Current Costs of Compliance for U.S. Businesses

What cost considerations are already top of mind for companies and legislators?[53] Aside from the obvious jurisdictional questions, inconsistency among state laws causes compliance difficulties for any company on the web, regardless if they are national or multinational. The existence of enforcement schemes and private rights of action vary across the board, and that lingering uncertainty leaves companies vulnerable to surprise costs.[54]

---

48. Dwight Weingarten, *House Members Renew Calls for Privacy Bill After Pandemic Pause,* MERITALK (July 13, 2020, 9:19 AM), https://www.meritalk.com/articles/house-members-renew-calls-for-privacy-bill-after-pandemic-pause/.

49. Rattigan, *supra* note 44 ("While the FTC was certainly busy under a Republican-led agency, it is likely that we will see a heightened level of scrutiny and more enforcement under a Biden-Harris administration. While Chairman Simons can serve until 2024, he might step down, and it is also likely that the FTC will gain more Democratic commissioners.").

50. Michael Volkov, *The Fundamental Gap in Data Privacy Enforcement*, VOLKOV: CORRUPTION, CRIME & COMPLIANCE (Oct. 29, 2020), https://www.jdsupra.com/legalnews/the-fundamental-gap-in-data-privacy-69621.

51. *See Id.*

52. *Id.* ("This issue usually divides Republicans and Democrats over whether to create another class action liability for companies that usually benefit plaintiff lawyers in organizing and prosecuting class action cases.").

53. Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND. (Aug. 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

54. *See* Lauren Fisher, *Privacy Year in Review: A Look Back at How 2019 Was a Preview of What's in Store in 2020*, EMARKETER (Dec. 16, 2019), https://www.emarketer.com/content/privacy-year-in-review-a-look-back-at-how-2019-was-a-preview-of-what-s-in-store-in-2020?_ga=2.257703630.477974023.1598237726-1283048191.1598237726 ("Already, 84% of US companies are complying with two or more privacy laws, with nearly half complying with six or more, according to an October 2019 poll of privacy professionals worldwide conducted by IAPP and TrustArc.").

GDPR disrupted the data privacy industry, and research has found that the cost of compliance with GDPR does not compare to the more extensive requirements of the newly amended CCPA.[55] Companies spend billions on GDPR compliance[56] but are forced to continuously rework these efforts as new legislation, like the CPRA, comes into effect, compounding their costs.[57] Putting all of the costs into perspective is a daunting task. In terms of the big picture, the Information Technology and Innovation Foundation (ITIF) explains,

> [I]f Congress were to pass legislation that mirrors many of the key provisions in the GDPR or the California Consumer Protection Act (CCPA), it could cost the U.S. economy approximately $122 billion, or $483 per U.S. adult, per year, which is more than 50 percent of what Americans spend on their electric bills each year. In contrast, if Congress passed a more targeted set of privacy protections, it could still boost consumer protection, but reduce costs by 95 percent to approximately $6.5 billion per year.[58]

In the meantime, state-level changes will continue to bear a massive cost burden on companies, which could be multiple times more expensive than current costs, as long as the federal government stalls on preemptive legislation and states continue to introduce their own unique frameworks. The cost of new federal data privacy legislation should be a top priority for lawmakers.

The unpredictable nature of such costs can have additional adverse effects on public companies, including liability in securities class actions that prioritize harm to shareholders, in addition to exposure to suits brought by consumers under statutes like the CPRA.[59]

---

55. Jehl & Friel, *supra* note 16.

56. The 2017 Privacy Governance Report by IAPP and EY found that Fortune's Global 500 companies will spend roughly $7.8 billion in order to ensure they are compliant with the EU General Data Protection Regulation. Mehreen Khan, *Companies Face High Cost to Meet New EU Data Protection Rules*, FIN. TIMES (Nov. 19, 2017), https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc.

57. *See* Amy He, *CCPA Is Here, But Many Companies Are Still Not Compliant*, EMARKETER (Jan. 3, 2020), https://www.emarketer.com/content/with-ccpa-days-away-many-companies-are-still-not-compliant ("According to August 2019 data from consent solutions provider PossibleNOW, 35% of US businesses polled said that they won't be CCPA compliant by January 1, 2020, because they feel it's too expensive to attain compliance.").

58. Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND. (Aug. 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

59. *See* Michael Lynch, Alysa Zeltzer Hutnik, & Rebecca Blake, *CCPA Litigation Update: How the CCPA (and other Privacy Risks) Raise the Risk of Potential Shareholder Claims,* AD LAW ACCESS (Oct. 30, 2020), https://www.adlawaccess.com/2020/10/articles/ccpa-litigation-update-how-the-ccpa-and-other-privacy-risks-raise-the-risk-of-potential-shareholder-claims/ (Detailing a securities class action suit, spurred by GDPR, where it is alleged that Facebook misled investors when it faced lower revenue after spending billions to comply with privacy standards, thus limiting the data users share with the company, in turn leading to reduced ad spend).

Over a third of American businesses did not expect to be fully compliant with the CCPA by its January 2020 effective date, primarily due to the high costs of compliance.[60] Although the more stringent requirements of the CPRA will not take effect until January 1, 2023, noncompliance with the CCPA can still result in fines of up to $7,500 per violation.[61] These fines could easily become six-figure expenses.[62] Some corporations process millions of pieces of personal data every single day. Consequently, even a series of undetected small violations could significantly affect their bottom line, and the aggregation of these losses may end up impacting the economy as a whole.

Companies' compliance costs can range from around $5 million per year to over $22 million dollars per year.[63] Expenses for specialized technology to facilitate compliance with data protection regulations make up the overwhelming majority of these costs.[64] Actual costs vary by organization size, but small organizations are disproportionately burdened, as per capita cost of compliance can be over eight times greater than for global corporations.[65] Meanwhile, corporations such as Microsoft, with market caps in the trillions,[66] cite proportionally lower billion-dollar figures when showcasing their cybersecurity expenses.[67]

---

60. *See* Erica Olson, PossibleNOW*Survey: As California Consumer Privacy Act Enforcement Approaches, 56% of Businesses Report They Will Not Be Fully Prepared,* CISION (Aug. 20, 2019), https://www.prweb.com/releases/possiblenow_survey_as_california_consumer_privacy_act_enforcement_approaches_56_of_businesses_report_they_will_not_be_fully_prepared/prweb16512360.htm (35% of respondents cited the cost of becoming compliant as the primary reason why their organization would not be compliant with the CCPA by January 1, 2020).

61. *See* CAL. CIV. CODE § 1798.155.

62. *See* He, *supra* note 57 ("Companies can be fined $2,500 for each record of unintentional violation and $7,500 for each record of intentional violation, which can add up to enormous sums for companies that are responsible for thousands or millions of data records.").

63. PONEMON INSTITUTE, GLOBALSCAPE, THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATION at 7 (2017). Though this pales in comparison to the cost of a breach, which is on average $4 billion, according to Ponemon Institute's 2016 Cost of Data Breach Study. *The Cost of Data Security: Are Cybersecurity Investments Worth It?*, CLOUDMASK, https://www.cloudmask.com/blog/the-cost-of-data-security-are-cybersecurity-investments-worth-it (last visited, Jan. 10, 2022).

64. PONEMON INSTITUTE, *supra note* 63, at 8 ("[C]ompliance costs relating to compliance technologies and incident response represent the two largest expenditure categories.").

65. *Id.* ("Figure 7 provides an analysis of total compliance cost on a per capita basis. When adjusted by headcount (size), compliance costs are highest for organizations with fewer than 1,000 employees and smallest for organizations with 75,000 or more employees.").

66. *See Microsoft Net Worth 2006-2021,* MACROTRENDS (last visited Jan. 4, 2022, 11:47 AM), https://www.macrotrends.net/stocks/charts/MSFT/microsoft/net-worth.

67. *See* Kim Crawley, *Cybersecurity Budgets Explained: How Much Do Companies Spend On Cybersecurity?,* AT&T CYBERSECURITY BLOG (May 5, 2020), https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget.

III. HOW CAN THE FEDERAL GOVERNMENT CREATE ECONOMIC EFFICIENCY WITH CENTRALIZED DATA PRIVACY REGULATIONS?

How long until consumers start to want more control over their data in the U.S.?[68] The federal government needs to get ahead of this inevitable movement for the sake of efficiency. Although compliance efforts will cost small businesses, the cost of compliance under multiple inconsistent state statutes is far more overwhelming.

What are the real concerns that data privacy laws aim to combat? Targeted consumer advertising that uses personal information bought and sold between corporations is becoming more of a concern for consumers.[69] Statistics show upward trends and positive movements in the privacy awareness of individuals in younger generations.[70] Average consumers know, or will eventually realize, that the mere fact that a company is legitimate, or that it is based in America, does not mean much for the protection of their personally identifiable information without some enforceable federal regulation. Only an omnibus federal law, strict enforcement of that law, and possibly a private right of action for citizens can provide appropriate protection for the general public.

In an ideal world, in addition to a federal private right of action, society needs preemption to streamline requirements for businesses of all sizes. The most realistic argument for preemption is that the field of data privacy is, in fact, already preempted by federal law, as it involves regulation of commerce within foreign states.[71] State regulation also burdens interstate commerce, meaning state laws are likely preempted by the Dormant Commerce Clause.[72] Although federal preemption is

---

68. EU citizens are generally increasingly more aware of their rights regarding their data since the implementation of GDPR. *See Your Rights Matter: Data Protection and Privacy: Fundamental Rights Survey*, EU FRA (2020), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf.

69. Brooke Auxier, et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. According to the Pew Research Center, a mere 6% of Americans believe that their data is more secure today. Pew also found that 81% of Americans believe the risks of companies' data collection outweigh the benefits. *Id.*

70. *100 Data Privacy and Data Security statistics for 2020*, DATA PRIVACY MANAGER: DATA PRIVACY BLOG, (Aug. 20, 2020), https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/ (noting that 61% of individuals who are active about their privacy are under the age of 45).

71. Andrea O'Sullivan, *Are California's New Data Privacy Controls Even Legal?,* REASON (Dec. 17, 2019),https://reason.com/2019/12/17/are-californias-new-data-privacy-controls-even-legal/(attempting to use state legislation rather than a federal solution raises serious constitutional problems involving the first amendment right to free speech and violations of the dormant commerce clause).

72. Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970); Jenny L. Colgate, *Does CCPA's Cross-Country Reach Render it Unconstitutional?,* LEXOLOGY, https://www.lexology.com/library/detail.aspx?g=fc597851-057a-45ae-a073-01ac4e4a6cd4. ("Under the second prong of the *Pike Balancing Test*, the Court considers whether the burden

expected by most experts in the field, the timing of such legislation is imperative. Requiring businesses to retool their data privacy and security compliance schemes repeatedly is costly, and this is an area where the new Biden administration has an opportunity to work swiftly to prevent redundancy.[73]

One option would be to use the F.T.C., which is already responsible for protecting consumers at a federal level.[74] Adding data protection to its mandate would be in line with its current consumer protection role.[75] The F.T.C. has taken some steps in this direction, like issuing guidances for companies on protecting consumer data.[76]

In light of the constitutional issues regarding preemption, the F.T.C. is an appealing candidate for the enforcement arm of federal data privacy legislation. Under the Dormant Commerce Clause and Foreign Commerce Clause, there can be an argument that states cannot regulate data and communications that cross state lines. An argument can also be made that the F.T.C. already has some authority here and has begun to exercise it.[77] Expanding the F.T.C.'s mandate explicitly, or at least giving it more funding, is one possible solution that could limit controversy, save start-up resources, and allow for a quicker implementation of the legislation.

The F.T.C. is also an attractive candidate because it is an independent agency, with commissioners appointed for seven-year terms.[78] The fact it is independent, with a built-in buffer to moderate changes in administration and parties controlling Congress, would provide a more stable and less partisan supervisor in charge of regulating data.[79]

So existing laws like the CCPA can be preempted by federal law, but what does the federal law that the F.T.C. would theoretically enforce look like? The E.U. regulates this area heavily, requiring companies to appoint Data Protection Officers and mandating extensive security

---

imposed by the state law on interstate commerce is clearly excessive in relation to the putative local benefits.").

73. It should be acknowledged that although this analysis takes place outside of a framework of currently existing federal omnibus legislation, if such a statute did exist, and included an express preemption clause, it would be presumed valid per *Puerto Rico v. Franklin Cal. Tax-Free Trust*. 136 S. Ct. 1938, 1946 (2016) (The Supreme Court "do[es] not invoke any presumption against pre-emption but instead focus[es] on the plain wording of the clause, which necessarily contains the best evidence of Congress' pre-emptive intent.").

74. One Agency, Two Missions, Many Benefits: The Case For Housing Competition And Consumer Protection In A Single Agency, 2014 WL 5616364 (F.T.C.).

75. *Id.*

76. Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance For Companies, Better Protection For Consumers,* FED. TRADE COMM'N: BUSINESS BLOG, (Jan 6, 2020 9:46 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

77. *See id.*

78. 15 U.S.C.A. § 41 (West 2022).

79. *See, Id.*

practices such as data mapping.[80] The CCPA goes even further in implementing strict, unlimited penalties relative to the size of the jurisdiction's economy.[81] At a minimum, the U.S. would need to have the same basic regulations as existing state laws, assuming cost remains a primary concern. The federal law will also require carve outs to avoid preempting existing specialized legislation by creating statutory exemptions in the new federal law for legislation such as child exploitation laws and HIPPA.

A federal standard saves big, national businesses money on compliance, but what about small businesses? The statutory definition of "small business" will be vital. Most "small" businesses avoid California's stringent compliance requirements because although the CCPA is extremely broad, it was initially intended to police data privacy and security practices of the most powerful corporations like Facebook, Google, and Amazon.[82] But as noted above, the importance of data privacy is trending up among consumers, and regulations from any other state could include these small businesses just the same. In sum, federal preemption could save small businesses where a company may be forced to fold if it lacks the necessary resources to overcome the inevitable future burden of conflicting state regulations.

It is also important to consider the rights that federal data protection legislation would provide the American people. Should a private right of action for consumers be a priority? It can be argued that individuals alone do not have enough bargaining power to pressure corporations into maintaining a functional response infrastructure, and S.E.C. style government actions or class action suits may be the only effective mechanism for enforcement.

Should the government be responsible for bringing civil or even criminal charges against violators? The CCPA requires that violations are brought in a civil action by the state attorney general.[83] Alternatively, the E.U. penalizes GDPR violators through administrative

---

80. *See,* Regulation (EU) 2016/679 of the European Parliament and 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. K 119/1.

81. ALICE MARINI ET AL., DATAGUIDANCE, & GABRIELA ZANFIR-FORTUNA ET AL., FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR VS. CCPA 37 (2019).

82. Therese Poletti, Opinion*: Regulating Big Tech Will be Hard, and California is Proving It*, MARKET WATCH: THERESE POLETTI'S TECH TALESARKET WATCH (Jan. 2, 2021 11:54 AM) https://www.marketwatch.com/story/the-push-to-regulate-big-tech-is-strongest-in-california-but-it-is-hitting-turbulence-11609430640.

83. CAL. CIV. CODE § 1798.100 (West 2020).

action.[84] GDPR's right to be forgotten[85] is most commonly cited by organizations as the most difficult type of GDPR compliance, because the cost of maintaining an infrastructure that allows for efficient processing of such requests is a significant investment. Is placing such a burden on companies the most efficient use of economic resources? Won't this merely proliferate into its own cottage industry?

The cost of providing a private right of action may very well be an insurmountable barrier for creation of a federal data privacy standard. Legislators need to consider and properly balance the need of consumers to exercise their rights freely versus the cost efficiencies that tasking an existing enforcement agency, like the F.T.C., can provide.[86]

IV. HOW CAN THE FEDERAL GOVERNMENT EFFECTIVELY ENFORCE OMNIBUS DATA PRIVACY LEGISLATION?

So, we have a national framework for compliance, how do we enforce this? A private right of action could create a consumer culture of empowerment, but such a right could also overwhelm an arguably less-than-tech-savvy judiciary and cause data protection costs for corporations to skyrocket.

HIPPA[87] is a successful federal enforcement model. It has widespread compliance without a private right of action, and state and federal enforcement is effective and sufficient to maintain compliance. This privacy provided by HIPPA is something American citizens have grown accustomed to and expect in their everyday lives. Credit bureau regulation is similar; the F.T.C. and C.F.P.B. enforce standards that have become so commonplace among consumers and businesses that it is hard to imagine a world without them.[88] Historically, enhancement in tort law has been used to protect consumers. The best example is the development of the law of strict liability for products put into the stream of commerce. But strict liability is generally applied in individual cases

84. Regulation 2016/679, of the European Parliament and 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. (L119) 32, 83.

85. IAPP & EY, ANNUAL GOVERNANCE REPORT 2019, 18 (2019)("Compliance with the 'right to be forgotten' still ranks first on the perceived difficulty scale . . .").

86. *See* 2020 FTC CONG. BUDGET JUSTIFICATION.

87. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.

88. *See generally* Hon. D. Duff McKee, *Liability for Wrongfully Furnishing or Obtaining a Credit Report Under the Federal Fair Credit Reporting Act*, 44 AM. JUR. PROOF OF FACTS 3D. 287 (Updated Dec. 2020) (discussing commonplace FTC regulations).

where someone has been hurt and suffered substantial injury.[89] Data breaches are happening, is a class-style $550 million payout enough?[90]

The most likely enforcement route will involve a federal agency. The F.T.C. is a suitable regulator of data because it has a history of cooperation with state regulators and consumer protection agencies, as well as foreign regulators, such as the European Commission of the E.U. and the U.K. Competition and Markets Authority, as well as the comparable agencies of major Asian countries: The Korean F.T.C., the Japanese F.T.C., and the Taiwan F.T.C.[91] Since the F.T.C. has international regulatory cooperation, it is a logical choice to lead an international effort.

This note has already highlighted the need to pivot from state-based data privacy standards to federal ones, further underscored by the indisputable fact that protecting data must be an international effort. Indeed, the internet is not a monolith, rather it is a worldwide network of interconnected data paths, tying together computing power and the data of millions of machines all over the world. Data flows seamlessly across national borders every second, and its regulation cries out for an international solution.

What regulatory scheme is most realistic in terms of enabling immediate enforcement standards? One way to quickly establish a regulatory system is to adopt the E.U.'s GDPR and adapt it to U.S. legal structures. If the purpose of federal preemption is to streamline national standards for the economic benefit of companies and consumers, it makes sense to consider a globally compatible approach as well.

The GDPR is applicable not just in the 27 countries of the E.U., but the additional four countries that make up the larger European Economic Area (EEA), Great Britain, Norway, Iceland and Liechtenstein.[92] This permits the U.S. to integrate with a working system. Further, the system is administered by the European Commission, which has a long history of cooperation with the F.T.C.

---

89. THEORIES OF LIABILITY: UNDERGROUND STORAGE TANK GUIDE § 1010 (Taylor Lewellyn, ed.) (Supp. Feb., 2019), Westlaw 13580288.

90. *Cf.* Kathleen Foody, *Unique Illinois Privacy Law Leads to $550M Facebook Deal*, ABC NEWS (Feb. 9, 2020), https://abcnews.go.com/Business/wireStory/unique-illinois-privacy-law-leads-550m-facebook-deal-68861584.

91. MOLLY ASKIN & RANDOLPH TRITELL, INTERNATIONAL ANTITRUST COOPERATION: EXPANDING THE CIRCLE, PRESENTATION AT THE ANTITRUST IN EMERGING AND DEVELOPING COUNTRIES CONFERENCE (Oct. 24, 2014), https://www.ftc.gov/system/files/attachments/key-speeches-presentations/141024 expandcircle-askin-tritell.pdf.

92. *Glossary: European Economic Area (EEA)*, EUROSTAT: STATISTICS EXPLAINED, https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European _Economic_Area_(EEA) (last visited Feb. 9, 2022).

The E.U. requires all corporations and other entities that do business there to abide by the GDPR.[93] In the internet era, even smaller companies can have business in the E.U. It is more efficient from a compliance—as well as an enforcement—perspective for businesses to apply the same rules to their U.S.-only clients as they apply to their international and EEA clients.

Moreover, combining the U.S. and EEA creates an enormous pool of people and industries. A platform of this size could then serve as a platform to add other major economies in Asia (Japan, South Korea, Taiwan, and Australia), as well as the Middle East and Indian subcontinent—or to become the foundation for a United Nations international treaty.

V. CONCLUSION

The current legislative landscape on data protection in the U.S. is fragmented and inefficient. Despite various federal efforts, American businesses and consumers are forced to navigate a constantly changing web of state and international regulations. The federal government should take ownership of this broken system to ease cost burdens and make consumer rights more easily accessible and identifiable.

The primary solution to standardizing data privacy legislation in the U.S. should come in the form of an omnibus federal law, preempting state laws while at the same time maintaining compatibility with current compliance regulations wherever possible. The F.T.C. is an ideal agency to implement an enforcement scheme because its established practices not only align with the mission of potential legislation, but also would present an efficient solution to regulating the cost of compliance and enforcement.

93. Regulation 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, 2016 O.J. (L 119) 87.