Campbell Law Review

Volume 45
Issue 1 *Fall 2022*

Article 4

2022

Consumer Data Privacy: A Federal Standard May Be the Cure for Business Compliance

Taylor M. Lammonds

Consumer Data Privacy: A Federal Standard May Be the Cure for Business Compliance

ABSTRACT

The discussion around personal privacy has only become more important in our modern, digitized world. In Europe, world leaders recognized the need for legal mechanisms to preserve personal data privacy in the wake of the Facebook Cambridge Analytica data scandal. Following suit in the United States, California and other States have passed their own legislation with similar laudable goals. However, the broad and sweeping effects of these laws means that businesses must shift resources from profitable uses into costly compliance regimes that, in some cases, are inconsistent with each other. This Comment discusses the burdens that these laws place on regulated businesses, as well as potential constitutional concerns. Finally, this Comment proposes that a federal standard be put in place in the United States to both ensure robust protection of consumers' personal data and to decrease the substantial burdens that a patchwork of state law creates for businesses that must comply with them.

INTRODUCTION

During every hour that a person spends using the Internet—whether scrolling through social media, online shopping, researching, or even just trying to find a recipe for dinner—data about that user is being created and collected. This data is not only immensely useful and necessary for the functioning of the Internet, but it is also a commodity. But the practices of the collection, use, and storage of this data have raised serious questions about whether the data is safe, what is being done with it, and the adequacy of mechanisms of control by persons the data describes. And the COVID-19 pandemic has only increased the importance of this issue. As working from home became the new norm, attending school online replaced the classroom, and video conferences replaced in-person meetings of all kinds, people have been required to spend more time on the Internet by new work protocols regarding video conferencing and remote-work platforms. These structural changes to interaction have caused consumer data to be shared and collected at unprecedented rates.

Even before the pandemic, the European Union (EU) was focused on these and other problems. In a comprehensive attempt to create a legal framework around data collection, the EU enacted one of the first laws to address these questions: the General Data Protection Regulation (GDPR).[1] The GDPR took effect on May 25, 2018, and was designed to protect consumers' data and privacy.[2] However, the broad scope of the law and the reach of the data it covered meant that business both inside and outside of the E.U. had to figure out both whether or not they fell under this new law and how it would affect them, creating broad-ranging compliance issues.[3]

Less than two years later, more business compliance issues surrounding consumer data privacy arose following the enactment of the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020.[4] The CCPA was designed to combat similar consumer protection issues in the data context as the GDPR. Businesses generally—but especially large, international businesses—then had to comply with both laws, each with its own protocols for compliance and varying punishments for

1. *See* Lindsay A. Seventko, *GDPR: Navigating Compliance as a United States Bank*, 23 N.C. BANKING INST. 201, 201 (2019).

2. *Id.*

3. *See generally Top Five Concerns with GDPR Compliance*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance [https://perma.cc/J45B-489S] (outlining five key reasons why organizations are concerned about GDPR compliance).

4. *CCPA vs CPRA: What's the Difference?*, BLOOMBERG LAW (July 13, 2021), https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/ [https://perma.cc/6WPE-X3Z9].

violations.[5] And the recent passage of other consumer privacy laws at the state level, such as the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (ColoPA), further added to compliance concerns. With the passage of these varying laws, not only must large, international businesses comply; smaller, domestic businesses must also comply.[6]

These recent legislative actions raise serious concerns for businesses. If businesses engaged in interstate commerce must comply with potentially fifty state variations on procedures regarding the wide-ranging nature of consumer data privacy—such as state-specific timelines for remedying violations enforced by hefty fines and sanctions—it is an inevitability that these businesses will be faced with conflicting demands and will be unable to effectively respond with compliance procedures that adequately protect consumers. Consumers will be harmed other ways, too: the more state laws conflict, the more they will effectively work a de facto transfer payment to insurance companies as errors and omission insurance premiums skyrocket. Further, the legal departments in companies, as well as hired law firms, may become paralyzed by processes and procedures and by remedying violations in each state once they inevitably occur.

To avoid these issues and protect both consumers and businesses a federal consumer privacy law with nationwide standards should be enacted. A federal law would more effectively protect consumers' data because businesses that use their data would be able to implement stronger policies and ensure compliance with a more uniform law. And consumer privacy issues will likely only grow in importance as personal information becomes accessible to more people and businesses than ever before.[7] Proactively implementing solid laws around these issues now is the best way to ensure the safety of consumers and businesses in the future.

This Comment will discuss the background of consumer data privacy laws in depth, beginning with the creation of the GDPR in the EU. The

5. *See generally* Sam Abadir, *CCPA's Top 5 Compliance Challenges*, NAVEX (Jan. 13, 2020), https://www.jdsupra.com/legalnews/ccpa-s-top-5-compliance-challenges-60336/ [https://perma.cc/U5W3-YM86] (addressing the top five challenges to complying with CCPA requirements); *see also Top Five Concerns with GDPR Compliance*, *supra* note 3.

6. *See generally Why We Need a National Privacy Law*, UNITED FOR PRIVACY, https://www.endtheprivacypatchwork.com/united-for-privacy#section3 [https://perma.cc/G4NV-D3ZM] (explaining the issues with the patchwork privacy laws); *see also* S. 569, 2021 Gen. Assemb. (N.C. 2021).

7. *See* Nicole Martin, *How Much Data is Collected Every Minute of the Day*, FORBES (Aug. 7, 2019, 3:34 PM), https://www.forbes.com/sites/nicolemartin1/2019/08/07/how-much-data-is-collected-every-minute-of-the-day/?sh=465ffce63d66 [https://perma.cc/9UPA-7RFN].

focus will then shift to the current consumer privacy legislation being passed and enacted in the U.S. California was the first state to enact a comprehensive consumer data privacy law, and other states, such as Virginia and Colorado, have followed California's lead.[8] However, this patchwork system has created problems which include general compliance issues for companies and even constitutional concerns. These laws, while important to protect consumer data, continue to be enacted in a haphazard way that overly burdens companies. This Comment proposes that Congress should enact a federal consumer data privacy law under its Commerce Clause power. A federal law will make compliance less burdensome on businesses that engage in interstate commerce because the rules will be uniform. This rids businesses of the challenging task of complying with, potentially, up to fifty different state laws regarding consumer data privacy.

I. THE CREATION OF THE GDPR

The GDPR took effect in the EU on May 25, 2018, and it was intended to protect consumers' data and privacy.[9] Specifically, it was designed to prevent data security issues such as the Facebook Cambridge Analytica data scandal[10] and to "provide a method of punishing companies with relaxed data security protocols by levying significant fines."[11] To achieve its desired goals of ensuring increased consumer data privacy, the GDPR focuses on "regulating in five main areas: (1) requiring companies to write privacy policies 'in clear, straightforward language'; (2) requiring companies to obtain 'an affirmative consent' from a user before the company can

8. Emily Catron & Gary Kibel, *Federal Data Privacy Legistation: Differences with State Laws Raise Preemption issues*, REUTERS (Aug. 10, 2022, 10:19 AM), https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10/ [https://perma.cc/B92F-GMSX].

9. Seventko, *supra* note 1, at 201–02.

10. The Facebook Cambridge Analytica data scandal arose after Cambridge Analytica harvested personal information from Facebook users. The information included where people lived and the pages that they liked. This data helped Cambridge Analytica build psychological profiles of Facebook users which allowed the company to analyze the users' "characteristics and personality traits." The information that was used to build these profiles of users ended up being deployed in political campaigns. Alexandra Ma & Ben Gilbert, *Facebook Understood How Dangerous the Trump-Linked Data Firm Cambridge Analytica Could be Much Earlier than It Previously Said. Here's Everything That's Happened up Until Now*, BUS. INSIDER (Aug. 23, 2019, 3:30 PM), https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3 [https://perma.cc/W43S-Y62C].

11. Seventko, *supra* note 1, at 201.

use the user's data; (3) encouraging companies to increase transparency on how and why consumer and user data is transferred, processed, and used in automated decision making; (4) giving [consumers and users] stronger rights over their data; and (5) giving the European Data Protection Board strong enforcement authorities."[12]

While the GDPR is a great step forward in the protection of consumer data, it has not come without consequences for businesses that access and possess consumer data. Businesses have faced compliance issues following the creation of the GDPR in five main ways: (1) businesses are required to increase "accountability, transparency and governance to minimize the risk of breaches" and must "adopt, test and maintain, and be prepared to demonstrate" their compliance to regulators; (2) businesses are required to adopt and maintain specific processes of internal data record-keeping, notifying regulators of "data breaches without undue delay[,]" and must appoint an "official Data Protection Officer"; (3) businesses face "[h]efty fines and sanctions" if they are unable to comply with the requirements of the GDPR; (4) businesses have to decipher vague requirements within the law such as the meaning of "undue delay" and "likelihood of (high) risk to rights and freedoms"; and (5) businesses around the world, not just in the EU, must be prepared to comply with the GDPR because of its extraterritorial reach.[13] While each of these five compliance issues create increased costs for businesses that use and access consumer data, arguably the biggest compliance impact of the law is its extraterritorial reach.

The territorial scope of the GDPR is sweeping in that it applies to the processing of personal data of a "controller or a processor in the Union . . . regardless of whether the processing itself takes place within the Union[;]" to the "processing of personal data of subjects who are in the Union by a controller or processor not established in the Union[;]" and to the processing of personal data by a "controller not established in the Union, but in a place where Member State law applies by virtue of public international law."[14] The GDPR views personal data as the property of the person and not the controllers or processors.[15] Thus, the GDPR applies to EU citizens no matter where they are in the world, regardless of whether

12. *Id*. at 202.

13. *Top Five Concerns with GDPR Compliance*, *supra* note 3.

14. 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 (General Data Protection Regulation) 2016 O.J. (L 119) 1, 4–5, 33 (EU) [hereinafter GDPR].

15. *See Top Five Concerns with GDPR Compliance*, *supra* note 3.

those controllers or processors actually operate within the EU.[16] Therefore, any business that deals with EU citizens' data, regardless of that business' location, will be subject to the requirements and the punishments laid out in the GDPR.[17] Consequently, because the use of technology and the Internet permeates every aspect of a person's life, it is "almost impossible" for any business that works with consumer data "to avoid dealing with some form of personal data from the European market."[18]

Although the GDPR created compliance issues due to its extraterritorial reach, once businesspersons realized that they would be subject to the GDPR requirements, it was possible to implement processes to avoid violations. And while it may have been time consuming and costly for those businesses to change protocols and processes to comply, GDPR was the only law of its kind regarding consumer privacy. In January of 2020 this changed when California's version of the GDPR, the CCPA, went into effect.[19]

II. THE CREATION OF THE CCPA AND THE CPRA

The CCPA became law on June 28, 2018, and it was designed to combat the same type of consumer privacy concerns as the GDPR.[20] The CCPA created an "array of consumer privacy rights and business obligations with regard to the collection and sale of personal information" and took effect one-and-a-half years after GDPR, on January 1, 2020.[21] While the CCPA and the GDPR share the objective of protecting consumer data, their varying compliance requirements have the potential to create confusion among businesses that must simultaneously comply with both of these relatively new laws.

The California State Legislature moved rapidly to pass the CCPA, leading some to criticize the law for being poorly drafted and for containing "terrible policy ideas."[22] The swiftness with which the law was passed allowed only minimal input from businesses affected by this law.[23] Technology companies criticize this law for impeding "innovation due to its

16. *See id*.

17. *See id*.

18. *Id*.

19. *CCPA vs CPRA: What's the Difference?*, *supra* note 4.

20. *Id*.

21. *Id*.

22. Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource"*, 93 S. CAL. L. REV. 99, 110 (2019) (quoting ERIC GOLDMAN, INTERNET LAW 357 (2019)).

23. *See id*.

stringent compliance requirements[,]" and they argue significant resources will be diverted from value-producing activities to "administrative and record-keeping tasks[,]" which is both economically and socially harmful.[24]

While the CCPA only applies to businesses meeting a specific set of criteria[25] (whereas the GDPR applies to businesses of every kind), it has introduced new regulations that have the potential to harm these businesses financially. The major compliance challenge businesses face in complying with the CCPA, as opposed to the GDPR, is the fact that the California law applies to a broader range of personal data. Under the CCPA, "personal information" includes any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[26] This definition of "personal information" is very broad, as it not only includes information that can be linked to an individual person, but also includes information that can be linked to households and devices.[27] Businesses will have to spend extra time and money to determine if some small amount of data collected *could* be linked to a person, their household, or their device, and how to monitor the collection of that data. It is estimated that the CCPA will lead to initial compliance costs of around $55 billion.[28] Over the next ten years, maintaining compliance could cost up to an additional $16 billion.[29] Small businesses are disproportionately affected by these compliance costs compared to bigger businesses that already had to comply with the GDPR because they will have to create their processes and protocols from scratch.[30]

Because of the criticism received for the errors resulting from its hasty drafting, the CCPA has since been amended. The amended law, the

24. *See id*. at 105.

25. To be required to comply with the CCPA, businesses must be for-profit and fall under at least one of the following characteristics: have "an annual gross revenue of more than $25 million;" collect, buy, sell, or share data of more than 50,000 consumers, devices, or households in California; or at least 50% of their annual revenue must come from selling this data. *Id.* at 107–08. And to be subject to the CCPA in the first place, businesses must also meet the following two criteria: They must (1) collect personal information from consumers in California and determine the purpose and "means of the processing of consumers' personal information"; and (2) do business in California. *Id*. at 107.

26. CAL. CIV. CODE § 1798.140(v)(1) (West 2022).

27. Kessler, *supra* note 22, at 111.

28. Jordan Yallen, *Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOY. L.A.L. REV. 787, 818 (2020).

29. *Id.*

30. *See id.*

California Public Records Act (CPRA), was approved by California voters on November 3, 2020, and will replace the CCPA when it takes effect January 1, 2023.[31] However, the CPRA does not solve all of the problems that businesses face regarding compliance because it "significantly amends and expands the CCPA[.]"[32] These expansions will force businesses that have only recently created protocols and processes for compliance with the CCPA to change those compliance processes again. Though many provisions of the CPRA are not likely to have a noticeable impact on businesses that must comply, some additions have the potential to create significant impact.

One of the most significant—and most troublesome—changes is how the CPRA will be enforced.[33] Under the CCPA, the Attorney General of California enforces the law, and businesses have a thirty-day cure period before being fined in the event of demonstrated noncompliance.[34] However, under the CPRA, a separate agency called the California Privacy Protection Agency (Protection Agency) has been created to replace the Attorney General's role in enforcement.[35] The Protection Agency is made up of a five-member board that has been given an initial budget of $10 million to help fund investigation and enforcement.[36] And not only is the Protection Agency now in charge of enforcement, but businesses no longer have a thirty-day period to cure noncompliance.[37] The removal of the security of the thirty-day cure period can be expected to cause additional resource reallocation because the fines for noncompliance are significant: each intentional violation carries a penalty of $7,500, and each unintentional violation is $2,500.[38]

Along with the new enforcement measures, there are a few other changes that have the potential to create major compliance problems for businesses. Under the CPRA, businesses are limited on the collection and retention of personal data[39]: Businesses can only retain data and infor-

31. Elizabeth Harding & Alex Polishuk, *CPRA—What This Means for Your Business*, JDSUPRA (Nov. 10, 2020), https://www.jdsupra.com/legalnews/cpra-what-this-means-for-your-business-36612/ [https://perma.cc/E24G-36NN].

32. *CCPA vs CPRA: What's the Difference?*, *supra* note 4.

33. *See CCPA vs. CPRA—What Has Changed?*, ONETRUST (Nov. 10, 2020), https://www.onetrust.com/blog/ccpa-vs-cpra-what-has-changed/ [https://perma.cc/5PHP-VMT5].

34. *Id.*

35. *See* CAL. CIV. CODE § 1798.199.10 (West 2022).

36. Harding & Polishuk, *supra* note 31.

37. *CCPA vs. CPRA—What Has Changed?*, *supra* note 33.

38. *Id.*

39. *See* Harding & Polishuk, *supra* note 31.

mation that is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed."[40] Also, businesses are required to inform consumers of the length of time that they intend to retain each category of the consumer's personal information.[41] The limitation on data retention is an issue for two reasons: first, because as a practical matter, it is time consuming and cumbersome to inform all consumers of the exact length of time their information will be stored. Second, and more important, the words "reasonably necessary and proportionate" are vague terms that open the door to violations and litigation regarding consumer data retention.[42] And at the same time the new requirements in the CPRA open the door for increased litigation, the CPRA expands the private right-of-action for consumers[43]: under the CPRA, consumers can bring claims against a business if an email address, password, or security question and answer that allows access into the consumer's account is breached.[44] This expands upon the CCPA's private right-of-action which only applies when the consumer's "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure" resulting from the business' failure to "maintain reasonable security procedures."[45]

The new private right-of-action, the vague language limiting data use, and the elimination of the thirty-day cure period all increase the risk of every inadvertent incident of noncompliance. Moreover, the Protection Agency will likely increase the number of investigations and enforcement actions as it is specialized and has increased resources and personnel.[46] Finally, businesses are more likely to have to defend litigation from numerous consumers in the event of a breach because of the expanded private right-of-action.[47] Laudable though the aims of CPRA are, these changes are likely to negatively impact a large proportion of businesses both financially and logistically.

And though California is the first state in the U.S. to implement strict consumer data privacy laws, it is not the last. With each new state privacy

40. *Id.*

41. *Id.*

42. *See id.*

43. *See CCPA vs. CPRA – What Has Changed?*, *supra* note 33.

44. *Id.*

45. CAL. CIV. CODE § 1798.150(a)(1) (West 2022).

46. *See* Chad Gross, *CPRA vs. CCPA: What's the Difference? 6 Key Changes to Understand*, A-LIGN (May 4, 2021), https://a-lign.com/cpra-vs-ccpa/ [https://perma.cc/63FB-BXUF].

47. *See* Harding & Polishuk, *supra* note 31.

law, interstate businesses will face increased costs and risks of noncompliance.

III. THE VIRGINIA AND COLORADO CONSUMER PRIVACY ACTS

Virginia and Colorado have recently passed their own consumer data privacy laws with similar objectives to both the GDPR and the CCPA/CPRA. On March 2, 2021, Virginia's then-Governor, Ralph Northam, signed the Virginia Consumer Data Protection Act (VCDPA).[48] This made Virginia the second state in the U.S. to enact a comprehensive state consumer data privacy law.[49] The VCDPA will go into effect January 1, 2023, and will apply to businesses that meet one of the following criteria: (1) the business controls or processes "personal data of at least 100,000 Virginia residents"; or (2) the business derives "over 50% of its gross revenue from the sale of personal data . . . and control[s] or process[es] data of at least 25,000 Virginia residents."[50] And not long after the passage of the VCDPA, on July 7, 2021, Colorado's Governor, Jared Polis, signed the Colorado Privacy Act (ColoPA) into law, and it will go into effect on July 1, 2023.[51] The ColoPA applies to businesses that intentionally target Colorado residents and that satisfy at least one of the following criteria: (1) they "control or process personal data of at least 100,000 consumers"; or (2) they "derive revenue or receive a discount on the price of goods and service[s]" from the sale of personal data or control the "personal data of at least 25,000 consumers."[52]

The VCDPA and the ColoPA are similar to the CPRA in that they all have been passed fairly quickly to accomplish the same general objective: to secure consumer data privacy for their residents.[53] However, the slight differences in these laws further complicate how businesses must comply. The VCDPA is enforced by the state Attorney General, and there is a thir-

48. Southwell, et. al., *Virginia Passes Comprehensive Privacy Law*, GIBSON DUNN (Mar. 8, 2021), https://www.gibsondunn.com/virginia-passes-comprehensive-privacy-law/ [https://perma.cc/HEU2-YGF8].

49. *See id*.

50. *Id.*

51. Aaron Burstein & Alysa Hutnik, *Privacy Law Update: Colorado Privacy Becomes Law: How Does it Stack Up Against California and Virginia?*, JD SUPRA (July 9, 2021), https://www.jdsupra.com/legalnews/privacy-law-update-colorado-privacy-5517597/ [https://perma.cc/7P6Z-KX5J].

52. *Id.*; Eddie Holman & Amanda Irwin, *Colorado Becomes Third State to Pass New General Privacy Law*, JD SUPRA, (June 30, 2021), https://www.jdsupra.com/legalnews/colorado-becomes-third-state-to-pass-5615105/ [https://perma.cc/AWJ6-HL3Q].

53. *See* Burstein & Hutnik, *supra* note 51.

ty-day right-to-cure period.[54] The ColoPA is also enforced by the state Attorney General and there is a sixty-day right-to-cure period, though the cure-period provision is set to be repealed on January 1, 2025.[55] These varying enforcement methods and right-to-cure periods portend the continuation of the patchwork approach to consumer data privacy, and their differences suggest that an optimal model for regulation is elusive.

Furthermore, the relatively rapid appearance of new laws indicates that state data privacy laws may continue to be passed. And though the sample size is small, there is a pattern of change in enforcement methods: as noted above, the CCPA allowed for a cure period and provided that the Attorney General would enforce the law, but soon after the law went into effect, the law was amended which deleted the cure period and changed the enforcement agency.[56] Similarly, the ColoPA has not even gone into effect, and the method of enforcement including the cure period is already set to be repealed and changed.[57] Both of these circumstances indicate that states have not been able to adequately assess the best method of enforcement *prior* to implementing the framework to be enforced. This uncertainty creates a burden on businesses because they cannot commit to solid compliance processes and protocols.

IV. CONSTITUTIONAL CONCERNS REGARDING PATCHWORK CONSUMER PRIVACY LAWS IN THE U.S.

While there are clearly business compliance concerns surrounding the enactment of each state's unique form of consumer data privacy laws, the concern does not stop there. With the rise of the patchwork system of consumer data privacy laws comes constitutional concerns. Specifically, there is concern that these laws may violate the Dormant Commerce Clause of the Federal Constitution because of their extraterritorial reach.[58]

One of the major compliance issues that initially arose from the creation of the GDPR was its extraterritorial reach. The creation of consumer privacy laws within the U.S. has led to similar concerns not only because these laws may not simply be hard to comply with but because they may be unconstitutional under the Dormant Commerce Clause.[59]

54. *See id*.
55. *Id.*
56. Harding & Polishuk, *supra* note 31.
57. Burnstein & Hutnik, *supra* note 51.
58. *See* Kessler, *supra* note 22, at 117.
59. *Id.*

Under the Commerce Clause of the United States Constitution, Congress has the power "[t]o regulate Commerce with foreign Nations, and among the several States[.]"[60] In *Gibbons v. Ogden*, Chief Justice Marshall introduced the idea of the Dormant Commerce Clause, which prohibits states from enacting laws that discriminate against or excessively burden interstate commerce.[61] Almost two hundred years later in *American Beverage Association v. Snyder*, the Dormant Commerce Clause concept was expanded upon when the Sixth Circuit Court of Appeals held that a state law which is not facially discriminatory will be per se invalid if the law "'directly controls commerce occurring wholly outside the boundaries of a State [and] exceeds the inherent limits of the enacting State's authority.'"[62] To determine if commerce is being controlled wholly outside of a certain state's boundary, a court must inquire as to whether the "'practical effect of the regulation is to control conduct beyond the boundaries of [that] State.'"[63]

While current consumer privacy laws in the U.S. are not facially discriminatory, they have the potential to control commerce wholly outside of the state in which they were enacted and have the potential to create an excessive burden on companies that participate in interstate commerce. As more and more states enact their own iteration of a consumer data privacy law with similar general objectives, in the aggregate, the variations in the compliance requirements imposed by the laws could very well be found to be significant.[64] If they are, these "disparate levels of compliance from companies that collect and process data from consumers in each state"[65] will arguably impose "substantial burdens" upon businesses and, as a result, upon interstate commerce.[66] Companies will have to "expend large sums of money" to comply, and as each state in the U.S. passes its own version of the law, the cost and resources dedicated to compliance may become overwhelming.[67]

However, the potential for excessive burden does not in itself create a Dormant Commerce Clause concern. For a law to create such an issue, the law must regulate commerce "wholly outside" of the state in which it

60. U.S. CONST. art. I, § 8, cl. 3.

61. Kessler, *supra* note 22, at 117 (citing Gibbons v. Ogden, 22 U.S. 1 (1824)).

62. Am. Beverage Ass'n v. Snyder, 735 F.3d 362, 373 (6th Cir. 2013) (quoting Healy v. Beer Inst., 491 U.S. 324, 336 (1989)).

63. *Id*. at 373.

64. *See* Kessler, *supra* note 22, at 117–18.

65. *Id*. at 118.

66. *See Why We Need a National Privacy Law*, supra note 6.

67. Kessler, *supra* note 22, at 118.

has been enacted.[68] While not every law will affect commerce wholly outside of the state, the laws enacted in large states, such as California, will almost certainly control business wholly outside of the state.[69] Businesses that primarily collect data outside of California, but do just enough business in California to require compliance with the CPRA, will have to comply with California's costly compliance demands.[70] Therefore, to comply with California law, a business will possibly have to use resources and funds that may have been allocated to business activities not at all involved in California, resulting in the law controlling how the business operates outside of the state.

The full extent of the potential issues relating to the Dormant Commerce Clause and the patchwork system of consumer privacy laws in the U.S. has yet to be seen. However, as more and more laws are enacted, the burden on interstate commerce will increase as businesses are forced to allocate large sums of money and resources to comply. And if, as has been the case so far, these laws continue to be passed and enacted quickly and with little input from the businesses that they will affect, the potential for excessive burden and direct control outside of the state will increase. There is a better way to protect consumer data and not place such an excessive burden on businesses to comply with varying state laws.

V. PROPOSAL FOR A FEDERAL CONSUMER PRIVACY LAW

The state-by-state approach to consumer data privacy laws in the U.S. is a cause for concern for both businesses and consumers.[71] In addition to the increased compliance expense for businesses as each state introduces its own law is the *implicit* risk that the web of procedures may result in less-than-adequate procedures and processes for protecting consumer data.[72] However, there is a way in which consumer data can be sufficiently protected without excessively burdening businesses, and that is by Congress enacting a federal consumer data privacy law.

Such a law has recently been introduced. Senator Jerry Moran, from Kansas, has introduced a bill to Congress entitled the Consumer Data Privacy and Security Act, which is essentially a consumer data privacy law that would set a clear federal standard for consumer data privacy protec-

68. *See Am. Beverage Ass'n*, 735 F.3d at 373.

69. *See Why We Need a National Privacy Law*, *supra* note 6.

70. *See id*.

71. *See* Sections III and IV, *supra*.

72. *See* Section II, *supra*.

tion.[73] The bill would preempt all previously enacted state laws, rules, and regulations regarding consumer data privacy and security.[74] It would specifically "take into account the limited size and resources of small businesses in determining their compliance[,]" which means that compliance requirements will be purportedly tailored to a business's capabilities.[75] Senator Moran's bill also provides the Federal Trade Commission (FTC) with necessary resources to enforce the law.[76] FTC enforcement would be "through targeted rulemaking[,]" and it would "issue first-time civil penalties for violations of the law."[77] The bill would also allow for state attorneys general to enforce the federal law.[78] A law similar to the one introduced by Senator Moran would greatly benefit businesses that must comply by giving them uniform compliance standards, "appropriately-scaled" requirements, and a uniform enforcement agency, each of which is likely to eliminate the confusion that the patchwork system has created.[79]

Though there could very well be pushback from the states, there is no doubt that Congress can regulate in this area pursuant to its Commerce Clause power.[80] The Commerce Clause provides that Congress has the power "[t]o regulate commerce with foreign Nations, and among the several States[.]"[81] And in *United States v. Darby*, the Supreme Court held that this power extends to all activity that substantially affects interstate commerce.[82] It is beyond dispute that the protection of consumer data privacy substantially affects interstate commerce given the amount of commerce that takes place through the Internet. Almost all companies that sell goods and services have an online presence, and most are interactive, meaning consumers can purchase the goods or services via the Internet. And even when consumers ultimately do not purchase a product online, it has been found that sixty-three percent of shopping occasions begin

73. *See* Press Release, Off. of Senator Jerry Moran, Senator Moran Introduces Bill Creating Clear Fed. Standard for Consumer Data Priv. (Apr. 29, 2021).

74. *See* Office of Senator Jerry Moran, *Consumer Data Privacy & Security Act*, https://www.moran.senate.gov/public/_cache/files/3/3/33d82198-546a-46db-bebc-ae09f566bbfa/699C2F4623FD95909912B9084A008E93.2021—-consumer-data-privacy-and-security-act—-moran.pdf [https://perma.cc/98KP-7UAE].

75. *Id.*

76. *See id.*

77. *Id.*

78. *Id.*

79. *Id.*

80. *See* U.S. CONST. art I, § 8, cl. 3.

81. *Id.*

82. Unites States v. Darby, 312 U.S. 100, 119–20 (1941).

online.[83] Many—perhaps even most—of the transactions that make up Internet commerce in the U.S. are not limited to parties within just one U.S. state, and products are daily sold and shipped throughout the nation.

Not only do consumers and businesses use the Internet to purchase and sell goods—transmitting their personal information in in the process—but their personal information itself, existing as data, is also a commodity to be bought and sold.[84] Many companies that collect consumer data will sell that data and work with third-party brokers to "gather information about a customer's behavior across multiple interactions with various entities[.]"[85] Even companies that do not outright sell data will share it with other companies or simply keep it for themselves as a way to learn consumer behavior and predict what consumers are likely to purchase.[86] Consumer data is a major commodity in the U.S. for both large and small businesses.[87]

The massive quantity of Internet commerce means that both because each time a person uses the Internet personal information is being collected about them and because that data itself is a product that can be bought and sold, the laws governing the privacy of that data have a clear, substantial impact on interstate commerce. Because of this, it is fully within Congress' power to regulate consumer data privacy laws.

The push for a federal law to create a uniform system of rules in a specific industry is not a novel idea. In 1938 for example, Congress passed, and former President Franklin Delano Roosevelt signed into law, the Food, Drug, and Cosmetic Act (FDCA) for the purpose of creating uniform regulations surrounding the using, selling, and advertising of food, drugs, and cosmetics.[88] The law put the Food and Drug Administration (FDA) in charge of enforcement,[89] and authorized the FDA to approve drugs as safe before they could be sold; prohibit false claims from drug manufacturers; mandate "legally enforceable food standards[,]" and

83. Maryam Moshin, *10 Online Shopping Statistics You Need to Know in 2021*, OBERLO (June 20, 2021), https://www.oberlo.com/blog/online-shopping-statistics [https://perma.cc/LBM9-ARLF].

84. *Your Data is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/9G7B-Z5CK].

85. *Id.*

86. *See id*.

87. *Id.*

88. *See Part II: 1938, Food, Drug, Cosmetic Act*, U.S. FOOD & DRUG ADMIN. (Nov. 27, 2018), https://www.fda.gov/about-fda/changes-science-law-and-regulatory-authorities/part-ii-1938-food-drug-cosmetic-act [https://perma.cc/7RM5-5L47].

89. *Id.*

formally authorize factory inspections.[90] The goal of the Act was to protect consumers from dangerous drugs, food, and cosmetics that were introduced and advertised as safe, but that in reality were dangerous.[91] By implementing a uniform set of regulations for companies to comply with, the FDCA was able to protect consumers by giving the businesses they purchased from a uniform standard to comply with.[92] This meant that businesses knew what they needed to do and were able to comply with the law in order to protect consumers.

And the same benefits would obtain here. A federally-established consumer data privacy law would create a uniform set of standards that would allow companies that collect personal data to enact strong compliance processes and procedures that will protect consumers without the transfer payments to insurance companies that a patchwork of laws necessarily requires.

While a federal consumer data privacy law would be constitutionally permissible, make business compliance easier, and result in stronger consumer protection, there is concern that if a federal law were to be introduced, it would essentially be a "watered-down" version of the currently enacted laws.[93] This is because in response to the enactment of the patchwork of laws, a few big technology companies, including Amazon, Google, Twitter, AT&T and Charter, have stated that they would contribute to and support the development of a federal consumer data privacy law.[94] The problem is that these "Big Tech" companies would likely oppose a law that is as strict as the GDPR or the CCPA and only support a more lenient law regarding consumer data privacy.[95] However, as more and more states enact their own versions of this law, technology companies may be more willing to compromise, because a stricter uniform law would be preferable to other laws with varying levels of compliance requirements.

There has also been concern regarding whether Congress would actually pass a federal consumer data privacy law. In 2012, the Obama Administration attempted to introduce the Consumer Privacy Bill of Rights to protect consumer data.[96] However, it was "met with strong opposition"

90. *Id*.

91. *See id*.

92. *See id*.

93. *See* Kessler, *supra* note 22, at 123.

94. *Id*. at 122–23.

95. *Id*. at 123.

96. *See* Press Release, Off. of the Press Sec'y, We Can't Wait: Obama Admin. Unveils Blueprint for a "Priv. Bill of Rts" to Protect Consumers Online (Feb. 23, 2012).

and lost momentum.[97] The Trump Administration did not attempt to enact any data privacy laws.[98] There has been a shift in momentum recently, and it seems that there is interest at the federal level around the issue.[99] The continuing introduction of similar laws in multiple states, as well as the federal bill introduced by Senator Moran earlier this year suggest that a federal consumer data privacy law could become a reality. And with increased pressure from businesses and consumers due to the current patchwork state of things, such a uniform law may yet be passed by Congress.

CONCLUSION

In nearly all of our interactions on the internet, personal information about us is collected. And as online interaction continues to increase, so too has the potential for misuse of this personal information. Recognizing this and following the example of the EU's enactment of the GDPR,[100] California enacted the CCPA to create a far-reaching legal framework to protect its citizens' data.[101] However, this latter law was hastily passed, creating compliance problems[102] that have only been exacerbated by the entry of two more states into the consumer privacy fray: Virginia and Colorado.[103] In the light of the issues caused by these overlapping regimes and to better protect the data of U.S. citizens, this Comment urges that Congress should pass a federal consumer privacy law under its Commerce Clause power.[104] A uniform federal law will standardize compliance procedures and protocols as well as enforcement for noncompliance, benefitting both businesses and consumers.[105]

---

97. Kessler, *supra* note 22, at 123.

98. *See id*.

99. On July 20, 2022, the American Data Privacy and Protection Act (ADPPA), H.R. 8152, was advanced to be introduced to the United States House of Representatives. The ADPPA is a bill intended to "create a comprehensive federal consumer privacy framework." *See* JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152, CONGRESSIONAL RESEARCH SERVICE 1 (Aug. 31, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776 [https://perma.cc/4LPR-9YVR]. This bill is bipartisan and was initially introduced by the House Energy and Commerce Committee. *Id.* While this bill has stronger backing than previous attempts to pass similar legislation, it is not clear as of this writing whether or not the bill will pass both houses of Congress.

100. *See* Section I, *supra*.

101. *See* Section II, *supra*.

102. *See id*.

103. *See* Section III, *supra*.

104. *See* Section V, *supra*.

105. *See id*.

Taylor M. Lammonds[*]

[*] J.D. Candidate 2023, Campbell University Norman Adrian Wiggins School of Law; B.A. Political Science, 2020, North Carolina State University. I would like to extend my gratitude to all of those who helped me throughout this process. First, I would like to thank my professor, the Honorable Zachary C. Bolitho, for his guidance and insight throughout the writing process. I would also like to thank the staff members and editorial board of Volume 45 of the Campbell Law Review for their hard work in helping me prepare and polish my Comment. Lastly, I would like to thank my friends and family, especially my husband, Brandon, for being patient with me and offering support during the long nights of writing and editing. Thank you to everyone who made all of this possible.