COMMENT

A NEW DIGITAL AGE: WHY COVID-19 NECESSITATES PREEMPTIVE FEDERAL ACTION TO REGULATE DATA PRIVACY*

I. INTRODUCTION

The arrival of COVID-19 in the United States created numerous issues related to data privacy and how companies collect, process, and store personal information. Starting in March 2020, the number of Americans engaging in the digital economy started to grow at record rates.[1] Naturally, this economic shift increased the volume of data that companies collected, processed, and stored.[2] In addition, most companies were forced to shift their employees to remote work environments, exposing companies to cybersecurity threats and breaches.[3] Employees who were permitted to work in the office often were required to provide personal healthcare information to their employer to protect against the spread of the virus.[4]

In the United States, data privacy protections are largely regulated at the state level.[5] While only California, Nevada, and Maine have passed data privacy laws, a majority of states have introduced data privacy legislation.[6] A state-by-state regulatory system would be extremely costly for multistate corporations forced to comply with potentially fifty

---

* Jason Hirsch, J.D. Candidate, Temple University Beasley School of Law, 2022. First, thank you to Juli Greenberg for her invaluable guidance and support. In addition, I thank the *Temple Law Review* staff for their thoughtful edits and comments. Finally, thank you to my family and friends for their unwavering love and support.

1. *See* Aamer Baig, *The COVID Recovery Will Be Digital: A Plan for the First 90 Days*, MCKINSEY (May 14, 2020), http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days [http://perma.cc/PT2X-BKTB] (explaining that the adoption of digital services has "vaulted five years forward . . . in a matter of . . . eight weeks").

2. *See id.*

3. *See Managing Cybersecurity and Data Privacy Concerns During the COVID-19 Pandemic*, JONES DAY: INSIGHTS (Apr. 2020) [hereinafter *Managing Cybersecurity*], http://www.jonesday.com/en/insights/2020/04/covid19-cybersecurity-and-data-privacy-concerns [http://perma.cc/CX3X-F2WN].

4. Laura E. Jehl & Deepali Doddi, *Privacy Considerations for COVID-19 Digital Contact Tracing*, NAT'L L. REV. (Sept. 29, 2020), http://www.natlawreview.com/article/privacy-considerations-covid-19-digital-contact-tracing [http://perma.cc/UW2G-3WRZ].

5. *See State Comprehensive-Privacy Law Comparison*, IAPP (July 6, 2020) [hereinafter *State Privacy Law Comparison*], http://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law.pdf [http://perma.cc/XVR7-RMYC].

6. *See infra* Part II.B.

unique data privacy laws.[7] In response to this concern, there is proposed federal legislation that would at least partially preempt state laws and provide the country with a uniform system of data privacy regulations.[8] If a federal data privacy law were enacted, it would provide significant cost savings for companies and eliminate the potential of inequitable protections between Americans residing in different states.[9]

Unfortunately, deep partisan divides in Congress have prevented meaningful action toward adopting a federal data privacy law. Since 2019, Congress has introduced a variety of bills that would govern the use of private data.[10] While the protections within each bill are substantively similar, there are nonnegotiable partisan differences in how each bill structures the scope of preemption, private right of action, and method of enforcement.[11] Ultimately, these disputes stalled efforts to enact a bill before 2021.[12]

This Comment provides recommendations for congressional policy that could effectively address the growing concern of data privacy in a post–COVID-19 world. Section II serves as an overview of the data privacy regulatory environment in the United States. In addition, Section II describes the data-related impacts of COVID-19 on Americans and companies doing business in the United States. Section III proposes a federal legislative approach to solving this problem. This policy proposal would enable Congress to achieve its goal of passing a federal data privacy law. For Congress to succeed, it must first regain Americans' trust to effectively regulate privacy before finding a bipartisan compromise over specific statutory disputes. Furthermore, Congress must adopt a forward-looking approach that forestalls future challenges.

II. OVERVIEW

This Section provides a general overview of the data privacy regulatory environment in the United States. In addition, this Section discusses concerns related to the COVID-19 pandemic and how those concerns uniquely impact the regulation and protection of personal data.

This Section proceeds in four parts. Part II.A outlines the California Consumer Privacy Act (CCPA)[13] and the recently passed California Privacy Rights Act (CPRA).[14] It also provides a comparative analysis of the CCPA and the European Union's General Data Protection Regulation (GDPR). Part II.B provides an overview on the range of different data privacy laws proposed and passed across the United States, focusing specifically on those of New York, Maryland, and Nevada. Part II.C discusses how

7. *See infra* Part II.B.

8. JONATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS 1 (2020), http://crsreports.congress.gov/product/pdf/LSB/LSB10441 [http://perma.cc/ZV9R-85DG].

9. *See* Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), http://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [http://perma.cc/HLD7-7R4T].

10. GAFFNEY, *supra* note 8, at 1.

11. *Id.*

12. *Id.* at 4.

13. California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2021).

14. California Privacy Rights Act of 2020, Proposition 24 (West) (to be codified at CAL. CIV. CODE §§ 1798.100–1798.199.100). The amendments will take effect in 2023.

Congress's inability to pass a federal data privacy law is driven by partisan disagreements about the scope of preemption and the creation of a private right of action. Finally, Part II.D will examine how the COVID-19 pandemic changed the way Americans and corporations view data privacy.

A. The CCPA, GDPR, and CPRA

The CCPA is the most comprehensive data privacy law in the United States.[15] Enacted on July 1, 2020,[16] the law marked a major shift from prior state data privacy regulations.[17] The CCPA is modeled partly on the GDPR[18] and sweeps into its grasp a diverse range of businesses with operations in California.[19] More importantly, the CCPA covers a regulatory area that lacks federal preemption and contributes to an increasing patchwork of data privacy laws that vary state to state.[20] On November 3, 2020, California voters approved a ballot initiative to expand the CCPA under the CPRA.[21] Beginning on January 1, 2023, the CPRA will broaden California consumer rights under the CCPA and establish a state oversight committee to enforce the law.[22]

While the CCPA has provided important protections for California residents' personal information, it has also created compliance challenges for businesses covered under the law.[23] According to a report commissioned by the California Department of Justice, the total cost of initial compliance with the CCPA was approximately $55 billion, which represented almost two percent of California's GDP in 2018.[24] Additionally, the

---

15. Rachael Myrow, *California Rings in the New Year with a New Data Privacy Law*, NPR (Dec. 30, 2019, 9:00 AM), http://www.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law [http://perma.cc/5GKQ-X3W3].

16. CAL. CIV. CODE § 1798.185(a) (West 2021).

17. ERIC N. HOLMES, CONG. RSCH. SERV., LSB10213, CALIFORNIA DREAMIN' OF PRIVACY REGULATION: THE CALIFORNIA CONSUMER PRIVACY ACT AND CONGRESS 1 (2018), http://crsreports.congress.gov/product/pdf/LSB/LSB10213/3 [http://perma.cc/R8ZK-XSB8].

18. *See* Sarah Hospelhorn, *California Consumer Privacy Act (CCPA) vs. GDPR*, VARONIS (June 17, 2020), http://www.varonis.com/blog/ccpa-vs-gdpr [http://perma.cc/X7T6-3W99]; DATAGUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA 8–9 (2018) [hereinafter DATAGUIDANCE], http://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [http://perma.cc/G8AH-GJZB].

19. *See* HOLMES, *supra* note 17, at 2.

20. Jennifer Huddleston, *Should Congress Be Concerned About California's Data Privacy Law?*, HILL (Dec. 3, 2019, 4:30 PM), http://thehill.com/opinion/technology/472834-should-congress-be-concerned-about-californias-data-privacy-law [http://perma.cc/V4DL-STQP].

21. Cynthia Cole, Matthew Baker & Katherine Burgess, *Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now*, BLOOMBERG L. (Nov. 16 2020, 4:00 AM), http://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now [http://perma.cc/DML6-BBQA].

22. *Id.*

23. *See* Mary Kraft, *Big Data, Little Privacy: Protecting Consumers' Data While Promoting Economic Growth*, 45 U. DAYTON L. REV. 97, 122 (2020).

24. DAVID ROLAND-HOLST , SAMUEL EVANS, DREW BEHNKE, SAMUEL NEAL, LIAM FRÖLUND & YAO XIAO, BERKELEY ECON. ADVISING & RSCH., LLC, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS 11 (2019),

CCPA's scope is limited to California residents, complicating compliance strategies for companies operating in multiple states.[25]

In order to understand the key challenges of legislating data privacy laws, Part II.A provides an overview on data privacy laws in both California and Europe. Parts II.A.1 and II.A.2 examine the nuances in the language of the CCPA. Part II.A.3 outlines the key differences between the CCPA and the European Union's data privacy law. Finally, Part II.A.4 details the key provisions of the CPRA and outlines how it differs from the CCPA.

1. CCPA Application

The purpose of the CCPA is to enforce transparent data practices and give California consumers more control over their personal information.[26] The CCPA applies to any "business" that collects the "personal information" of "consumers."[27] While consumer is defined as "a natural person who is a California resident,"[28] its definition extends broadly to contacts from business customers, employees, or other businesses that reside in California.[29]

"Business" includes any for-profit company that collects personal information of Californians, does business in California, and satisfies at least one of the following thresholds: (1) earns more than $25 million in annual gross revenues; (2) "annually buys, receives for the business' commercial purpose, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"; or (3) "[d]erives 50 percent or more of its annual revenues from selling consumers' personal information."[30]

"Personal information" is broadly defined. The term can be linked to any information that "identifies, relates to, describes, [or] is reasonably capable of being associated with" a California consumer or household.[31] This link can be either direct or indirect.[32] The statute defines personal information to include browsing history, search history, and other information a company can gather from a user's interaction with a website.[33] In addition, the scope includes any "inferences drawn" from this information.[34] The CCPA provides exemptions for some categories of personal information, including information lawfully made available from government records and "deidentified" or "aggregate consumer information."[35]

---

http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf [http://perma.cc/K8BQ-L8GP].

25. *See* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.140(g) (West 2021).

26. Assemb. B. 375, 2017-18 Reg. Sess., § 2 (Cal. 2018) (enacted).

27. CAL. CIV. CODE § 1798.105(a).

28. *Id.* § 1798.140(g).

29. 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, 811–12 (2020).

30. CAL. CIV. CODE § 1798.140(c)(1)(A–C).

31. *Id.* § 1798.140(o)(1).

32. *Id.*

33. *Id.* § 1798.140(o)(1)(F).

34. *Id.* § 1798.140(o)(1)(K).

35. *Id.* § 1798.140(o)(2)–(3).

The CCPA provides consumers with three main "rights" to control their personal information: the right to know, the right to opt out, and the right to delete.[36] First, the CCPA grants consumers the right to know what personal information is collected about them.[37] In advance, businesses must inform California consumers about the categories of personal information being collected and how that information will be used.[38] A business must also disclose upon request specific pieces of personal information collected or sold, the categories of sources from which the information was collected, and any third parties the information was shared with.[39] The consumer may request disclosure of information at any time; however, a business is only required to provide an individual consumer with her personal information twice every twelve months.[40]

Second, the CCPA provides consumers the right to opt out of the sale of personal information.[41] Businesses must inform consumers of this right and cannot sell the consumer's information to third parties unless the consumer provides the business with express authorization to do so.[42] In addition, the CCPA prohibits a third party from selling purchased personal information unless the consumer received notice and an opportunity to opt out.[43]

Third, consumers have the right to request that a business delete his or her information.[44] When a business receives this request, it must delete the information collected within forty-five days (with possible extensions of an additional forty-five or ninety days) and direct its "service providers" to do the same.[45] There are a few narrow exceptions to this right, including when the information is needed to complete a particular transaction for the consumer, to detect security-breach incidents, or to ensure that another consumer can exercise free speech rights.[46]

2. CCPA Enforcement

The California Attorney General enforces the CCPA.[47] Businesses that violate the CCPA and do not cure the violation within thirty days may incur civil penalties of up to $7,500 per violation.[48] Private causes of action are only available for a consumer whose "nonencrypted and nonredacted personal information" is subject to "unauthorized access and exfiltration, theft, or disclosure."[49] The consumer must provide the business thirty

36. HOLMES, *supra* note 17, at 3.

37. *Id.*

38. CAL. CIV. CODE § 1798.100(b).

39. *Id.* § 1798.110(a)(1)–(5).

40. *Id.* § 1798.100(d).

41. HOLMES, *supra* note 17, at 3.

42. *Id.*

43. CAL. CIV. CODE § 1798.115(d). The CCPA also gives minors the right to opt in by affirmatively authorizing a business to sell their personal information. Consumers between thirteen and sixteen years of age may opt in themselves but consumers under thirteen must be opted in by their parent or guardian. *Id.*

44. HOLMES, *supra* note 17, at 3 (referring to this right as the "right to delete").

45. CAL. CIV. CODE § 1798.130(a)(2).

46. *Id.* § 1798.105(d)(1)–(4).

47. *Id.* § 1798.185(c).

48. *Id.* § 1798.155(b).

49. *Id.* § 1798.150(a)(1).

days written notice and an opportunity to cure the violation before bringing suit for a CCPA violation.[50] Consumers may recover damages of no less than $100 and no more than $750 "per incident," or actual damages, whichever is greater.[51] Finally, the CCPA created a Consumer Privacy Fund, where twenty percent of all civil penalties or proceeds from a settlement action are deposited to offset costs incurred by the government.[52]

3. Comparing the GDPR and CCPA

The European Union was the first jurisdiction to enact legislation protecting the rights of consumers' personal information.[53] The GDPR went into effect on May 25, 2018, and updated an outdated data privacy law enacted over twenty years earlier.[54] In response to the GDPR, dozens of states (including California) began to propose their own data privacy laws.[55] While the CCPA and GDPR were proposed and enacted to enhance consumer data privacy protections, the CCPA substantially deviates from the GDPR with respect to scope, consumer rights, and enforcement.[56] These differences likely generate additional compliance costs for any company that engages in business in both California and the European Union.[57]

a. Differences in Scope

The GDPR has a much broader scope than the CCPA.[58] Unlike the CCPA—which only regulates for-profit entities—the GDPR covers all businesses, public bodies, and institutions, including not-for-profit organizations.[59] While the CCPA only protects consumers who are California residents, the GDPR does not require residency or citizenship to qualify for its protections.[60]

The GDPR covers organizations that do not have any presence in the European Union but offer goods, services, or monitor the behavior of persons in the European Union.[61] In contrast, the CCPA only applies to entities that do business in California.[62]

---

50. *Id.* § 1798.150(b).

51. *Id.* § 1798.150(a)(1)(A).

52. *Id.* § 1798.155(c).

53. Elizabeth L. Feld, *United States Data Privacy Law: The Domino Effect After the GDPR*, 24 N.C. BANKING INST. 481, 481 (2020).

54. *The History of the General Data Protection Regulation*, EUROPEAN DATA PROT. SUPERVISOR, http://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [http://perma.cc/7836-49EF] (last visited May 1, 2022).

55. *See infra* Part II.B; Feld, *supra* note 53, at 490.

56. DATAGUIDANCE, *supra* note 18, at 5.

57. *See* Feld, *supra* note 53, at 483.

58. *See* Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BAKER HOSTETLER LLP, http://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf [http://perma.cc/W4LD-85BQ].

59. 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, art. 4, 2016 O.J. (L 119) 1, 33–35 [hereinafter General Data Protection Regulation].

60. *See* Jehl & Friel, *supra* note 58.

61. General Data Protection Regulation, *supra* note 59, at art. 3.

62. California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.140(c) (West 2021).

Unlike the GDPR, the CCPA does not expressly apply to businesses established outside of California.[63] However, based on the California Franchise Tax Board's definition of "doing business in California," it appears that out-of-state entities collecting, selling, or disclosing the personal information of California residents are within the CCPA's scope.[64]

The material scopes of the GDPR and the CCPA are broad.[65] However, unlike the GDPR—which does not exclude specific categories of personal information from its protections—the CCPA provides several categorical personal information exceptions. These exceptions include medical information, publicly available information, employee information, and personal information covered by other sector-specific legislation (such as the Gramm-Leach-Bliley Act).[66]

b. Differences in Consumer Rights

The scope of consumer protections under the CCPA differs in numerous regards compared to the GDPR.[67] The right to opt out of sales of personal information to third parties is covered by both the GDPR and CCPA.[68] However, unlike the CCPA, the GDPR does not include a specific right to opt out of sales of personal data.[69] In addition, the GDPR does not require the covered entity to include an opt-out link on a website homepage.[70] While the GDPR does not include a specific right to opt out, it does contain other rights that protect consumers, including the ability to opt out of processing data for marketing purposes and the ability to withdraw consent for processing activities.[71]

While the GDPR's and the CCPA's deletion rights are similar,[72] the GDPR provision governing deletion rights only applies to businesses if the deletion request meets one of six conditions.[73] In contrast, the CCPA allows businesses to refuse deletion requests on broader grounds than the GDPR.[74] The GDPR requires deletion requests to be replied to within one month from the receipt of the request, which can be extended to two additional months depending on the complexity and number of requests.[75] This timeline differs from the CCPA, which enforces a forty-five-day deadline to respond to a deletion request with a forty-five- or ninety-day extension period.[76]

---

63. DATAGUIDANCE, *supra* note 18.

64. *Id.*

65. *See* Jehl & Friel, *supra* note 58.

66. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified primarily at 15 U.S.C. §§ 6801–6809, §§ 6821–6827); *see also* DATAGUIDANCE, *supra* note 18, at 7–12.

67. *See* Jehl & Friel, *supra* note 58.

68. *See id.*

69. *See id.*

70. *See* DATAGUIDANCE, *supra* note 18, at 30–32.

71. *See* Jehl & Friel, *supra* note 58.

72. The right to delete provides the consumer the option to delete personal information a business collects. *See id.*

73. General Data Protection Regulation, *supra* note 59, at art. 17.

74. *See* Jehl & Friel, *supra* note 58.

75. General Data Protection Regulation, *supra* note 59, at art. 12.

76. *See* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.130(a)(2) (West 2021).

Finally, the GDPR provides consumers with additional rights that the CCPA does not.[77] First, the GDPR grants consumers the right to correct inaccurate or incomplete personal data.[78] Second, the GDPR grants consumers the right to restrict processing of personal data under certain circumstances.[79] Third, the GDPR grants consumers the right to object to processing for profiling; direct marketing; and statistical, scientific, or historical research purposes.[80] Fourth, the GDPR grants consumers the right not to be subject to automated decisionmaking.[81]

c. Differences in Enforcement

Both the CCPA and the GDPR contain provisions that enable private causes of action and subject covered entities to monetary penalties for civil damages.[82] However, the nature of the penalties, the amount, and the procedure for both laws have substantial differences.[83] The GDPR authorizes administrative fines of up to four percent of global annual turnover or €20 million, whichever is higher.[84] The amount of the penalty depends on a number of factors, including the nature, gravity, and duration of the infringement; the nature of the processing; the number of consumers affected; and the actual damages suffered.[85] In contrast, the CCPA's civil penalty regime is simpler, imposing $2,500 for each violation and $7,500 for each intentional violation.[86]

The GDPR allows private causes of action to be brought for any violation of the law,[87] while the CCPA only permits private causes of action when unencrypted or nonredacted personal information is subject to an unauthorized access as a result of a data breach.[88] In addition, while the GDPR does not provide a range for potential damages, the CCPA is more specific in limiting the amount of damages from private causes of action.[89]

4. The California Privacy Rights Act

Even as companies begin to acclimate to the CCPA's regulatory scheme, the Act will not last long in its current form.[90] The CPRA, a ballot initiative, was approved by California voters in the 2020 elections.[91] While the CPRA's provisions will not be enforceable until January 1, 2023, the Act significantly changes the scope and

77. *See* Jehl & Friel, *supra* note 58.
78. *See id.*
79. *See id.*
80. *See id.*
81. *See id.*
82. *See* DATAGUIDANCE, *supra* note 18, at 37.
83. *Id.*
84. *See* General Data Protection Regulation, *supra* note 59, at art. 83(5).
85. *See id.* at art. 83(2).
86. *See* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.155(b) (West 2021).
87. *See* General Data Protection Regulation, *supra* note 59, at art. 82.
88. *See* CAL. CIV. CODE § 1798.150(a)(1).
89. DATAGUIDANCE, *supra* note 18, at 37–40.
90. *See* Cole et al., *supra* note 21.
91. *See id.*

enforcement of the existing law and expands the consumer rights of California residents.[92]

First, the CPRA limits the scope of the CCPA by doubling the threshold requirement to qualify as a "business" from 50,000 to 100,000 consumers or households.[93] On the other hand, the CPRA creates a more strictly protected category of "sensitive personal information," which includes government-issued identifiers, account credentials, financial information, and precise geolocation.[94] Under the CPRA, covered entities that process this sensitive personal information would be subject to additional regulations and restrictions.[95] The CPRA also creates a new oversight committee to enforce the law, named the California Privacy Protection Agency.[96] The Agency will be governed by a five-member board and replace the enforcement powers currently held by the California Attorney General.[97] Businesses covered under the law "must perform annual cybersecurity audits" and submit regular risk assessments to the California Privacy Protection Agency.[98]

The CPRA will also expand consumer rights. California consumers would have the right to "(1) [c]orrect personal information; (2) [k]now the length of data retention; (3) [o]pt-out of advertisers using precise geolocation [data]; and (4) [r]estrict usage of sensitive personal information."[99] Finally, the CPRA will expand the private right of action penalty to include unauthorized access or disclosure of an email address and password if the business fails to take appropriate security precautions.[100]

B. Expansion of State Data Privacy Laws

As of September 2021, twenty-one states have introduced data privacy bills seeking to protect consumers' personal information.[101] The bills differ from state to state, with some proposing broader consumer protections than the CCPA,[102] and others proposing significantly narrower protections.[103] Without federal oversight, this diverse data privacy regulatory environment at the state level has the potential to create a fragmented system

92. *See* Kathryn M. Rattigan, *New California Privacy Rights Act on the 2020 Ballot*, NAT'L L. REV. (Sept. 11, 2020), http://www.natlawreview.com/article/new-california-privacy-rights-act-2020-ballot [http://perma.cc/HMH4-NWNA].

93. Kyle Levenberg & F. Paul Pittman, *Before the Dust Settles: The California Privacy Rights Act Ballot Initiative Modifies and Expands California Privacy Law*, JD SUPRA (Nov. 17, 2020), http://www.jdsupra.com/legalnews/before-the-dust-settles-the-california-40451/ [http://perma.cc/FTU4-EQQZ].

94. Rattigan, *supra* note 92.

95. *See id.*

96. *Id.*

97. *Id.*

98. Levenberg & Pittman, *supra* note 93.

99. Rattigan, *supra* note 92.

100. *Id.*

101. *See State Privacy Law Comparison*, *supra* note 5.

102. *See, e.g.*, S.B. 5642, 2019–2020 Leg., Reg. Sess. § 1103 (N.Y. 2019).

103. *See, e.g.*, S.B. 220, 2019 Leg., 80th Sess. § 1 (Nev. 2019).

of laws.[104] This Part discusses two state proposals and one enacted state law that illustrate the wide range of provisions at the state level.

Part II.B.1 discusses the proposed New York Privacy Act,[105] a bill that would apply broad protections to consumers' personal data. Part II.B.2 reviews Maryland's proposed Online Consumer Protection Act,[106] which would provide similar consumer protections as the CCPA. Part II.B.3 outlines Nevada's enacted data privacy law, SB-220.[107] Finally, Part II.B.4 provides an explanation of the costs of a state-by-state regulatory approach.

1. New York: New York Privacy Act

The New York Privacy Act (NYPA) is significantly broader than the CCPA and, if enacted, will establish the broadest state law protections to consumers over their personal data in the United States.[108] The NYPA contains a few similarities to the CCPA. The NYPA grants consumers the right to know what data companies are collecting, provides consumers a right to delete or correct personal data, and allows consumers to opt out of having their data sold to third parties.[109]

However, the NYPA significantly departs from the scope and protections of the CCPA. First, the NYPA does not impose a minimum revenue or consumer threshold for businesses.[110] Some scholars and politicians believe that eliminating the revenue threshold will expose small companies to compliance costs.[111] Second, the NYPA imposes a fiduciary obligation to consumers.[112] This obligation supersedes any duty owed to owners or shareholders of a covered entity.[113] For public companies that also owe a duty to shareholders, the NYPA will create difficult and costly decisions when shareholders' interests do not align with New York law.[114] Third, along with the opt-out provision, the NYPA allows consumers to affirmatively opt in to use of their personal data.[115]

---

104. *See* Emily Tabatabai, Heather Sussman, Nicholas Farnsworth & Sulina Gabale, *State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills*, ORRICK (Mar. 19, 2019), http://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills/ [http://perma.cc/7QNB-F4EX].

105. S.B. 6701A, 2021–2022 Leg., Reg. Sess. (N.Y. 2021).

106. S.B. 957, 2020 Gen. Assemb., Reg. Sess. (Md. 2020).

107. S.B. 220, 2019 Leg., 80th Sess. (Nev. 2019).

108. *See* Issie Lapowsky, *New York's Privacy Bill Is Even Bolder Than California's*, WIRED (June 4, 2019, 7:00 AM), http://www.wired.com/story/new-york-privacy-act-bolder/ [http://perma.cc/96P5-CE4H].

109. *See* Rory Bennett, *What To Expect if the New York Privacy Act Is Enacted, Following the Privacy Regulation Boom of GDPR and CCPA*, INFO. AGE (Mar. 11, 2020), http://www.information-age.com/what-to-expect-new-york-privacy-act-enacted-123488202/ [http://perma.cc/5EN2-4WFS].

110. Viola Trebicka, Serafina Concannon & Sophia Qasir, *Inside the Proposed New York Privacy Act*, LAW.COM (Sept. 2, 2020, 11:21 AM), http://www.law.com/newyorklawjournal/2020/09/02/inside-the-proposed-new-york-privacy-act/ [http://perma.cc/7T4A-YEC5].

111. *See id.*

112. *See* S.B. 5642, 2019–2020 Leg., Reg. Sess. § 1102 (N.Y. 2019).

113. *See id.*

114. *See* Trebicka et al., *supra* note 110.

115. *See* N.Y.S.B. 5642 § 1103.

Finally, the NYPA expands the private right of action beyond the limits set by the CCPA.[116] Under the NYPA, a right of action can be brought by "any person who has been injured by reason of a violation of this article."[117] As long as actual harm can be shown, a consumer can sue a covered entity for any violation of the Act.[118] Unlike the CCPA, which only allows a private right of action for violations related to certain types of private information, the NYPA will allow a private right of action for all violations of the statute.[119]

2. Maryland: Online Consumer Protection Act

Maryland's Online Consumer Protection Act (OCPA), introduced in early 2020, both expands and narrows certain consumer rights as compared to the CCPA.[120] The OCPA contains similar protections as the CCPA but imposes slightly more limited disclosure obligations on businesses.[121] In addition, the OCPA does not include a private right of action for consumers.[122]

Other provisions of the OCPA broaden consumer protections compared to the CCPA.[123] For example, under the OCPA's right-to-opt-out provision, companies are required to disclose information passed to third parties regardless of whether the information was sold.[124] The CCPA's opt-out provision is narrower, applying only to information *sold* to a third party.[125] Finally, the OCPA goes beyond the CCPA's opt-in provision for minors by completely prohibiting the disclosure of information of consumers under the age of eighteen.[126]

3. Nevada: SB-220

Nevada's data privacy law, SB-220, was enacted in 2019 (prior to the CCPA) and provides substantially narrower data privacy protections than the CCPA.[127] Unlike the CCPA, SB-220 does not provide consumers with a right to access personal information, a right to request deletion of personal information, or the opportunity to raise a private right of action against a covered entity.[128] SB-220 also applies only to operators of

116. *See* Trebicka et al., *supra* note 110.

117. N.Y.S.B. 5642 § 1109(3).

118. *See id.*

119. *See* Trebicka et al., *supra* note 110.

120. *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Apr. 2, 2021), http://www.varonis.com/blog/us-privacy-laws/ [http://perma.cc/6F75-HSR6] (reviewing numerous federal and state privacy laws).

121. Tabatabai et al., *supra* note 104.

122. *Id.*

123. *Id.*

124. *Id.*

125. *See id.*; *see also supra* Part II.B.1.

126. Tabatabai et al., *supra* note 104.

127. *See* Alexandra Scott & Lindsey Tonsager, *Nevada's New Consumer Privacy Law Departs Significantly from the California CCPA*, COVINGTON (June 10, 2019), http://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa/ [http://perma.cc/B935-ZNWK].

128. *See id.*

websites and online services, not to offline business operations.[129] While SB-220 contains an opt-out provision resembling that of the CCPA, it applies to a narrower scope of personal information and does not require a "Do Not Sell" button on the homepage of a website.[130] Finally, SB-220 provides businesses less time to respond to consumer requests to opt out (a maximum of 90 days including extensions compared to the CCPA's maximum of 135 days).[131]

4. Requirements for Compliance with State Laws

Each state's unique privacy laws complicate the patchwork of laws with which entities must comply.[132] Critics of this state-by-state approach express concerns related to the significant compliance costs companies would incur to properly navigate numerous unique data privacy laws.[133] This concern has already manifested along the Nevada-California border, where many companies are forced to comply with two differing sets of data privacy laws.[134] As states continue to introduce and enact data privacy legislation, state-by-state compliance obstacles will naturally become more commonplace.[135]

C. Congressional Attempts To Enact a Federal Data Privacy Law

Since 2019, the U.S. Congress has recognized the economic and practical issues with a fragmented, state-level data privacy regulatory scheme.[136] As of late 2021, twelve bills have been introduced in Congress that would provide a comprehensive federal data privacy framework.[137] While there is bipartisan support in Congress for a federal data privacy law, three issues have frustrated efforts to pass legislation: (1) whether state privacy laws should be expressly preempted, (2) whether to include a private right of action for consumers, and (3) whether the Federal Trade Commission (FTC) should be the federal agency that enforces corporate compliance practices.[138] As of late 2021, partisan politics has caused congressional deadlock regarding preemption and the private rights of action. However, there is some tentative bipartisan agreement over the FTC's enforcement responsibilities.[139]

---

129. *Id.*

130. *See id.*

131. *See id.*

132. *See* Beckerman, *supra* note 9.

133. *See id.*

134. *See id.*

135. *See id.*

136. *See* GAFFNEY, *supra* note 8, at 1.

137. *See* Megan Brown, Boyd Garriott, Duane Pozza & Kathleen Scott, *Federal Privacy Law Efforts Move Forward in Congress*, JD SUPRA (Oct. 5, 2020), http://www.jdsupra.com/legalnews/federal-privacy-law-efforts-move-19243 [http://perma.cc/DJW7-RJ8G]; GAFFNEY, *supra* note 8.

138. Yallen, *supra* note 29, at 788–99.

139. Jessica Davis, *Senate GOP Bill Proposes Federal Privacy Standard Bill, Preempts States*, XTELLIGENT HEALTHCARE MEDIA (Mar. 13, 2020), http://healthitsecurity.com/news/senate-gop-bill-proposes-federal-privacy-standard-bill-preempts-states [http://perma.cc/5QCK-KELB].

1. The Issue of Preemption

The extent of federal preemption presents a major obstacle for Congress.[140] Republicans have proposed legislation that expressly preempts currently enacted state laws.[141] They believe this broader approach to preemption would create uniform data privacy laws, lower compliance costs for corporations, and eliminate state-level data protection inequities for consumers.[142]

For instance, the SAFE DATA Act,[143] introduced by Senator Wicker (R-MS) in September 2020, would preempt all state laws "related to the data privacy or data security and associated activities" of covered entities.[144] This broad preemptive language would sweep away existing state privacy legislation, including the CCPA and SB-220.[145]

In contrast, Democrats have proposed legislation that will only preempt state law when it conflicts with a federal provision.[146] Democratic leaders claim this narrower approach to preemption is justified by concerns that express preemption would not provide enough protections to consumers.[147] In addition, Democrats argue that setting a preemptive floor would allow states to pass stricter privacy laws to protect consumers.[148] Some scholars claim that while this solution would not solve the issues of uniformity and rising corporate compliance costs, it would promote statutory flexibility in a rapidly changing digital environment.[149]

For instance, the Consumer Online Privacy Rights Act (COPRA),[150] introduced by Senator Cantwell (D-WA) in November 2019, would only preempt "directly conflicting" state laws, preserving significant parts of existing state statutes.[151] In addition, COPRA's preemptive impact excuses state laws which "[afford] a greater level of protection."[152]

2. The Issue of a Private Right of Action

Another congressional split focuses on whether federal data privacy legislation should permit a private right of action.[153] Republican-sponsored bills, including the

140. Cameron F. Kerry & John B. Morris, Jr., *Preemption: A Balanced National Approach to Protecting All Americans' Privacy*, BROOKINGS: TECHTANK (June 29, 2020), http://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy/ [http://perma.cc/8TBH-GEFD].

141. *Id.*

142. *See* Davis, *supra* note 139.

143. S. 4626, 116th Cong. (2020). This bill would establish data privacy and data security protections for consumers in the United States. *Id.*

144. *Id.* § 405(a).

145. Kerry & Morris, *supra* note 140.

146. *See* GAFFNEY, *supra* note 8, at 4.

147. *See* Kerry & Morris, *supra* note 140.

148. *See id.*

149. *See id.*; Henry Adams, *The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action*, 84 MO. L. REV. 1055, 1092–94 (2019).

150. S. 2968, 116th Cong. (2019); GAFFNEY, *supra* note 8, at 4.

151. *See* S. 2968 § 302(c).

152. Kerry & Morris, *supra* note 140.

153. GAFFNEY, *supra* note 8, at 4.

SAFE DATA Act, do not include a private right of action provision.[154] Republicans believe that providing a private right of action would cause disproportionate harm to smaller companies and put a heavy burden on enforcement agencies.[155] In contrast, Democratic-sponsored bills, including COPRA, have included a private right of action provision that significantly broadens consumers' right to sue covered entities.[156] Under COPRA, as long as there is a violation of the statute, a private suit can be brought.[157] This strict liability provision reflects other privacy-related legislation, including the Telephone Consumer Protection Act[158] and the Video Privacy Protection Act.[159] In addition, COPRA allows for liquidated damages, punitive damages, and recovery of attorney's fees.[160]

Proponents of a broad private right of action justify their position in two ways. First, they argue that individuals should be allowed to seek compensation for legally protected privacy interests.[161] Second, proponents assert that a private right of action would induce compliance by supplementing other modes of enforcement.[162]

Opponents of a private right of action acknowledge that individuals should have a right to redress;[163] however, they are more concerned about preventing frivolous litigation.[164] In addition, opponents assert that the inclusion of a private right of action increases the potential for class action lawsuits that would expose companies to damages regardless of the claim's merits.[165] Finally, opponents claim COPRA's broad private right of action mandate would violate the Constitution's standing requirements.[166]

---

154. Brown et al., *supra* note 137.

155. Lauren Feiner, *A Federal Privacy Law Is Starting To Crystallize, But Democrats and Republicans Can't Agree on How To Do It*, CNBC (Dec. 4, 2019), http://www.cnbc.com/2019/12/04/a-federal-privacy-law-is-starting-to-crystallize-senators-remain-divided-over-details.html [http://perma.cc/3SP6-USK5].

156. *See id.*; Kerry & Morris, *supra* note 140.

157. Megan L. Brown & Kathleen E. Scott, *Congress Accelerates Year End Privacy Efforts, With Remarkable Agreement and Differences on Preemption and Private Rights of Action*, WILEYCONNECT (Dec. 5, 2019), http://www.wileyconnect.com/home/2019/12/5/congress-accelerates-year-end-privacy-efforts-with-remarkable-agreement-and-differences-on-preemption-and-private-rights-of-action [http://perma.cc/LG8B-JX6J].

158. 47 U.S.C. § 227(b)(3)(B).

159. 18 U.S.C. § 2710(c).

160. Brown & Scott, *supra* note 157.

161. Cameron F. Kerry & John B. Morris, *TechTank: In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition*, BROOKINGS (July 7, 2020), http://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/ [http://perma.cc/TS66-L5CS].

162. *Id.*

163. *See id.*

164. Brown et al., *supra* note 137.

165. Kerry & Morris, *supra* note 161.

166. *See* WILSON C. FREEMAN, CONG. RSCH. SERV., LSB10303, ENFORCING FEDERAL PRIVACY LAW – CONSTITUTIONAL LIMITS ON PRIVATE RIGHTS OF ACTION 1 (2019), http://fas.org/sgp/crs/misc/LSB10303.pdf [http://perma.cc/JSJ5-JTHW]; *see infra* notes 167–169 and accompanying text.

Case law also impacts Congress's ability to incorporate effective statutory language for the private right of action. In *Spokeo Inc. v. Robins*,[167] the plaintiff alleged that Spokeo, Inc. illegally harvested personal data in violation of the Fair Credit Reporting Act.[168] The Supreme Court of the United States concluded that the plaintiff failed to establish standing, which requires showing "a concrete, particularized, and actual or imminent injury-in-fact."[169] Skeptics of COPRA's private right of action provision assert that since COPRA would not require consumers to show an injury-in-fact before filing a claim, plaintiffs suing under the law could fail to meet the standing precedent the Supreme Court set in *Spokeo*.[170]

3. The Issue of Enforcement Authority

The final issue facing Congress is federal data privacy legislation enforcement.[171] Since mid-2020, there has been increasing bipartisan support for an enforcement provision providing the FTC the authority to enforce consumer privacy protections.[172] The SAFE DATA Act would provide the FTC and state attorneys general the authority to enforce federal consumer privacy protections.[173] Similarly, COPRA would establish an enforcement agency inside the FTC.[174] Entrusting the FTC with enforcement responsibilities would likely be effective because the Commission has already been addressing various data privacy concerns.[175]

While an FTC enforcement provision has gained broad support in Congress, a proposed bill, the Data Protection Act (DPA), offers an alternative enforcement structure.[176] The DPA would create a new agency to oversee data privacy protections.[177] Unlike the FTC, which is constrained by other regulatory mandates, a new agency would have the latitude to operate in rapidly developing digital markets not covered by the FTC.[178] However, there are concerns that creating a new agency would add to the already oversized administrative state.[179] While the DPA's enforcement provision has some appeal, the bill has not gained traction in Congress.[180] Without a significant ideological

167. 136 S. Ct. 1540 (2016).

168. FREEMAN, *supra* note 166, at 2.

169. *Id.*

170. *See* Joseph Jerome, *Private Right of Action Shouldn't Be a Yes-No Proposition in Federal US Privacy Legislation*, IAPP (Oct. 3, 2019), http://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation/ [http://perma.cc/9RAR-QRR5].

171. GAFFNEY, *supra* note 8, at 4.

172. Davis, *supra* note 139.

173. *Id.*

174. *Id.*

175. *See* Jennifer Huddleston, *A Primer on Data Privacy Enforcement Options*, AM. ACTION F.: INSIGHT (May 4, 2020), http://www.americanactionforum.org/insight/a-primer-on-data-privacy-enforcement-options/ [http://perma.cc/L84V-UP8D].

176. *Id.*

177. *Id.*

178. *Id.*

179. *Id.*

180. *See id.*

shift in Congress following the 2022 elections, an FTC enforcement provision will likely remain the preferred statutory policy going forward.

D. COVID-19's Impacts on Data Privacy Concerns

The COVID-19 pandemic has drastically shifted how companies, consumers, and lawmakers approach data privacy.[181] Companies have digitalized their operations to protect employee health and provide services to quarantined customers.[182] This sudden shift toward a predominantly digital economy increased consumer concerns about online collection of personal information.[183] Additionally, the collection of confidential healthcare data for contact tracing introduced issues that exposed the private information of millions of Americans.[184] While lawmakers have responded to COVID-19 privacy concerns by proposing two bills focused on contact-tracing data privacy,[185] it is unlikely that any federal legislation will be passed in the near future.[186]

1. Corporate Response to COVID-19

The COVID-19 pandemic significantly impacted the digital economy.[187] As a result of the pandemic, time spent at home increased, resulting in a dramatic shift in consumer behavior.[188] The number of online consumers is expected to further increase by as much as forty percent.[189] In addition, it is likely that a majority of people using digital channels for the first time will continue to use them even after the pandemic.[190]

This shift in consumer behavior prompted companies to expand and create new digital services.[191] Banks transitioned to remote sales and services teams, while grocery

---

181. Jack Dunn, *Defining a 'New Normal' for Data Privacy in the Wake of COVID*-19, IAPP (Jun. 16, 2020), http://iapp.org/news/a/defining-a-new-normal-for-data-privacy-in-the-wake-of-covid-19/ [http://perma.cc/5T3T-YYQU].

182. *See* Baig, *supra* note 1.

183. *The Cost of Privacy: Reporting on the State of Digital Identity in 2020*, OKTA [hereinafter *The Cost of Privacy*], http://www.okta.com/cost-of-privacy-report/2020/ [http://perma.cc/5YFP-8UNW] (last visited May 1, 2022).

184. Jehl & Doddi, *supra* note 4.

185. Mimi Nguyen, *Federal Privacy Law in Response to COVID-19 on the Rise: The COVID-19 Consumer Data Protection Act of 2020 vs. the Public Health Emergency Privacy Act*, JD SUPRA (June 5, 2020), http://www.jdsupra.com/legalnews/federal-privacy-law-in-response-to-26186/ [http://perma.cc/47ZL-VYW3].

186. *See* David Uberti, *Coronavirus Privacy Bills Hit Roadblocks in Congress*, WALL ST. J. (June 15, 2020, 3:19 PM), http://www.wsj.com/articles/coronavirus-privacy-bills-hit-roadblocks-in-congress-11592213400 [http://perma.cc/WBB6-RHJZ].

187. *COVID-19: The Unexpected Catalyst for Tech Adoption*, NIELSEN: INSIGHTS (Mar. 16, 2020), http://www.nielsen.com/us/en/insights/article/2020/covid-19-the-unexpected-catalyst-for-tech-adoption/ [http://perma.cc/65SV-QEGF].

188. *See* Jeremy Carlson & Hyunjin Kim, *Survey: US Consumer Sentiment During the Coronavirus Crisis*, MCKINSEY (Oct. 7, 2020), http://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/survey-us-consumer-sentiment-during-the-coronavirus-crisis [http://perma.cc/3DNQ-NSJK].

189. *See id.*

190. Baig, *supra* note 1.

191. *See id.*

stores built a digital infrastructure to accommodate online ordering and delivery.[192] The retail industry adjusted to the logistical challenges of an increased volume of online sales.[193] Overall, data has shown that the digital economy accelerated five years forward in consumer and business digital adoption in the first two months of the pandemic.[194] As the infrastructure for digital services expands, so too will the amount of personal data collected by companies providing these services.[195] Without proper regulatory guidance, companies need to independently assess the sensitivity of the additional personal information collected.

COVID-19 also created internal corporate data privacy concerns. For many companies, a large percentage of their workforce began working from home.[196] As a result, companies reviewed and revised privacy policies to ensure that employees' personal data and other confidential information remained secure.[197] Still, COVID-19 caused heightened cybersecurity risks arising from the surge of remote work.[198] Businesses experienced an uptick in social engineering schemes aimed at encouraging employees to open COVID-19–related messages infected with malware.[199] While federal agencies—such as the Cybersecurity and Infrastructure Security Agency and the FTC—issued cybersecurity guidance, companies still face data privacy issues without unified regulatory guidance.[200]

Another privacy challenge for companies is the collection of health data from employees to ensure that they are healthy before returning to the office. The Equal Employment Opportunity Commission (EEOC) released guidelines that allow employers to collect employees' sensitive healthcare information as long as that information is "job-related and consistent with business necessity."[201] In addition, all medical information collected must be kept confidential and be treated as a medical record.[202]

---

192. *See id.*

193. *See* Akrur Barua & Monali Samaddar, *A Recovery in Retail Sales Is Underway Amid COVID-19, but There Are Challenges Ahead,* DELOITTE: INSIGHTS (Sept. 25, 2020), http://www2.deloitte.com/us/en/insights/economy/spotlight/economics-insights-analysis-09-2020.html [http://perma.cc/4HAA-27AT].

194. *See* Baig, *supra* note 1.

195. ORG. FOR ECON. CO-OPERATION & DEV., DATA IN THE DIGITAL AGE (2019), http://www.oecd.org/ [http://perma.cc/P3AA-FG93].

196. *See Managing Cybersecurity*, *supra* note 3.

197. *See* Casey Ross, *After 9/11, We Gave Up Privacy for Security. Will We Make the Same Trade-off After Covid-19?*, STAT (Apr. 8, 2020), http://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/ [http://perma.cc/EWB4-CEGK].

198. *See* Glenn A. Brown & Shalin R. Sood, *Business in the Time of COVID-19: US Cybersecurity and Privacy Issues for You To Consider*, NAT'L L. REV. (Mar. 24, 2020), http://www.natlawreview.com/article/business-time-covid-19-us-cybersecurity-and-privacy-issues-you-to-consider [http://perma.cc/FCD2-RGWL].

199. *Managing Cybersecurity*, *supra* note 3.

200. *See id.*

201. *Pandemic Preparedness in the Workplace and the Americans with Disabilities Act*, U.S. EQUAL EMP. OPPORTUNITY COMM'N [hereinafter EEOC, *Pandemic Preparedness*], http://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act [http://perma.cc/Z65S-FRRW] (last visited May 1, 2022).

202. *Id.*

While the EEOC guidelines cover employee health data privacy during the pandemic, there is no guidance directing companies in how to use this data after the pandemic ends.[203]

Finally, large tech companies, such as Google and Apple, began working with the U.S. government to use app-enabled geolocation features and facial-recognition technology to better understand how the virus is spreading.[204] The data was anonymous and aggregated, allowing the government to analyze the patterns of spread without knowing an individual's movements.[205]

2. Consumer Concerns

While the onset of COVID-19 augmented consumer concerns about personal data, a large proportion of Americans are still not aware of how or when their data is being collected and used.[206] Forty-two percent of Americans do not think online retailers collect data about their purchasing histories, and thirty-five percent of Americans are unaware of efforts to track the spread of COVID-19 through smartphone data collection.[207] Furthermore, six in ten Americans know very little or nothing at all about the laws and regulations currently in place to protect their data privacy.[208]

While most Americans are not aware of how their data is being used, eighty-six percent worry their data will be used for purposes other than COVID-19.[209] In addition, eighty-one percent are worried their data will be used to serve advertisements to them.[210] Even if consumers were offered money for their personal data, most value privacy over extra cash.[211] It is clear that since the pandemic, most Americans became more concerned about the collection of their personal data.[212] However, with companies collecting an increasing volume of personal information, there are added concerns that many Americans will still fail to recognize whether their personal information is being used for unauthorized purposes.[213]

Data collection during COVID-19 also implicates balancing the security of the population against the privacy of personal information collected to track and test sick

---

203. *See id.*

204. *See* Jeffrey L. Turner, *Privacy vs. Security in the Post-Pandemic World*, NAT'L L. REV. (June 12, 2020), http://www.natlawreview.com/article/privacy-vs-security-post-pandemic-world [http://perma.cc/63B2-DB4S].

205. Brown & Sood, *supra* note 198.

206. *The Cost of Privacy*, *supra* note 183.

207. *Id.*

208. Brooke Auxier, *How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak*, PEW RSCH. CTR.: FACTTANK (May 4, 2020), http://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/ [http://perma.cc/7TXU-DMKL].

209. *The Cost of Privacy*, *supra* note 183.

210. *Id.*

211. *See id.*

212. *See id.*

213. *See* Auxier, *supra* note 208 (explaining that while most Americans were concerned about how companies were using their personal data, only six percent knew a great deal about how their data was being handled).

Americans.[214] This balance between security and privacy is a recurring issue in American politics and is premised on the question of whether someone is willing to give up liberty to receive additional protection from the government.[215] Based on data collected prior to the pandemic, a majority of Americans said they benefited very little or not at all from the data companies and the government collected about them.[216] Although the benefit of collecting confidential data for contact tracing and testing increased,[217] Americans still valued their data privacy over those public health benefits of contact tracing efforts.[218] A 2020 poll suggests that a majority of Americans were not willing to expose their personal data to public or private entities for the purpose of contact tracing.[219] In addition, six of ten Americans think location tracking through cellphones would not make a difference in limiting the spread of COVID-19.[220]

Without laws that regulate pandemic-related healthcare and consumer data, many experts fear Americans' trust in government will continue to erode.[221] As of 2020, American trust in their government's ability to safely handle personal data is lower than in other developed nations.[222] At the same time, seventy-five percent of Americans say that there should be more government regulation of personal data than there is right now.[223] The longer Congress fails to act, the more likely it is that Americans will lose faith in the government's ability to protect their personal data.[224]

3. Congressional Proposals To Address COVID-19

In response to the COVID-19 pandemic, Congress proposed two bills to address the collection of sensitive healthcare data. Republican senators introduced the COVID-19 Consumer Data Protection Act of 2020 (CCDPA),[225] which would require the FTC to obtain affirmative, express consent from individuals prior to collecting, processing, or transferring their personal health, geolocation, or proximity information for the purposes of contact tracing.[226] In addition, companies would be responsible for informing consumers at the point of collection how data will be handled, while permitting consumers to opt out of the collection process.[227] Under the CCDPA, companies would also be responsible for deleting or de-identifying personally

214. *See* Turner, *supra* note 204.

215. *See id.*

216. *See The Cost of Privacy*, *supra* note 183.

217. *See* Beth Duff-Brown, *Model Shows Potential Contact Tracing Impact Against COVID-19*, STAN. MED. (Aug. 24, 2020), http://med.stanford.edu/news/all-news/2020/08/model-shows-potential-contact-tracing-impact-against-covid-19.html [http://perma.cc/DYM6-AJ98].

218. *See The Cost of Privacy*, *supra* note 183.

219. *Id.*

220. Auxier, *supra* note 208.

221. *See The Cost of Privacy*, *supra* note 183.

222. *Id.*

223. Auxier, *supra* note 208.

224. *See id.*

225. S. 3663, 116th Cong. (2020).

226. Nguyen, *supra* note 185.

227. *Id.*

identifiable information once it is no longer used for COVID-19 purposes.[228] Like other Republican-sponsored data privacy bills,[229] the CCDPA would expressly preempt any state law that relates to the collection, processing, or transfer of covered data for the purpose of COVID-19 contact tracing and social distancing.[230] Finally, the CCDPA does not include a private right of action against covered entities that violate the bill.[231]

Senate Democrats introduced the Public Health Emergency Privacy Act (PHEPA)[232] in response to the CCDPA.[233] Like other Democratic-sponsored data privacy legislation,[234] PHEPA contains a narrower preemption mandate than the CCDPA and grants a private right of action for violations that constitute a concrete and particularized injury in fact.[235] Unlike the CCDPA, which only applies to covered entities that are not already covered by the Health Insurance Portability and Accountability Act (popularly known as HIPAA),[236] PHEPA includes governmental use, collection, and disclosure of emergency health data under its purview.[237] PHEPA also contains a broader ban on certain collections, uses, and disclosures of emergency health data.[238] Under PHEPA, emergency health data used for commercial advertising, e-commerce recommendations, or e-commerce and advertising algorithms are prohibited.[239]

Both the CCDPA and PHEPA reflect key data privacy policy differences that Congress is unlikely to resolve in a timely fashion.[240] Disagreements regarding the scope of preemption and the private right of action will likely stall any progress of both bills, which ultimately imposes compliance costs on companies and possibly exposes consumers' personal healthcare data to unconsented third-party usage.[241]

III. DISCUSSION

COVID-19's disruption of the digital economy brought about new ways for companies to collect personal information to the detriment of consumers.[242] While state legislatures have acted to pass privacy measures to protect individuals' personal data, a state-level system is not the solution.[243] Until Congress passes a federal data privacy law,

228. *Id.*

229. *See supra* Part II.C.

230. Nguyen, *supra* note 185.

231. *Id.*

232. S. 3749, 116th Cong. (2020).

233. Nguyen, *supra* note 185.

234. *See supra* Part II.C.

235. Nguyen, *supra* note 185.

236. H.R. 3103, 104th Cong. (1996).

237. Nguyen, *supra* note 185.

238. Junaid Odubeko & Andrew Tuggle, *A Second Privacy Bill for COVID-19 Has Larger Scope, More Enforcement*, BRADLEY (May 19, 2020), http://www.bradley.com/insights/publications/2020/05/a-second-privacy-bill-for-covid19-has-larger-scope-more-enforcement [http://perma.cc/YLJ5-LS5K].

239. *Id.*

240. *See* Uberti, *supra* note 186.

241. *See* GAFFNEY, *supra* note 8, at 4.

242. *See* Jehl & Doddi, *supra* note 4.

243. *See* Beckerman, *supra* note 9.

both citizens and companies will suffer from the inequities of a fragmented system of state laws.

Initially, the federal government must prioritize certain policy initiatives before proposing a new data privacy legislation. Part III.A discusses four ways Congress can regain Americans' trust in the federal government's ability to regulate personal data. First, Congress must prioritize data privacy over increased public health and safety surveillance. Second, Congress should establish federal programs to educate Americans on how and when their data is being collected and processed. Third, Congress must ensure that personal data with the potential to be processed or sold to third parties will be protected. Finally, Congress must consider disruptive technological advances impacting the integrity and effectiveness of the law.

Part III.B argues that Congress must also consider the financial burden a data privacy law would place on companies. If the law's scope is too broad, companies will incur high compliance costs. Alternatively, if the law's scope is too narrow, many of the complexities associated with a fragmented state-by-state regulatory system will remain. While Congress should prioritize privacy protections, it must keep in mind the cost to regulated companies.

Even if Congress follows through on the overarching policy initiatives discussed in Parts III.A and III.B, partisan issues remain for specific statutory provisions. Part III.C examines solutions to the congressional deadlock over preemption and private right of action. Finally, Part III.D discusses why a data privacy law should include provisions addressing public health–specific issues such as contact tracing, employers' collection of employee healthcare data, and the increased volume of cybercrimes impacting U.S. companies and citizens.

A. Rebuild Americans' Trust in the Federal Government

In order for Congress to enact and enforce a federal data privacy bill, Americans must believe that Congress will pass effective legislation addressing relevant data privacy concerns. Currently, seventy-one percent of Americans have limited to no trust in the government's ability to regulate personal data.[244] As a result, members of Congress will find it challenging to support a bill handing over the power of data privacy enforcement to the federal government.

Congress *can* regain Americans' trust in the federal government's ability to regulate personal data. To do so, there must be substantial efforts to assure Americans that a federal privacy law will have an effective, long-lasting impact on the protection of personal data.

Congress should refer to important privacy-related lessons learned after the September 11, 2001, attacks on the World Trade Center. Following September 11, Congress took aggressive action to protect the safety of Americans.[245] As a result, government surveillance was left largely unregulated to protect against domestic terrorist attacks.[246] While this policy had widespread support in the early 2000s, it lost its public

244. *The Cost of Privacy*, *supra* note 183.

245. *See* Turner, *supra* note 204.

246. *See id.*

appeal as the internet and smartphones became more prominent across society.[247] Eventually, support for this "security first" policy subsided in 2013 when Edward Snowden revealed widespread government surveillance of U.S. citizens.[248] Since 2013, public trust in the federal government's ability to regulate privacy collapsed,[249] contributing to federal inaction and a fragmented system of state privacy laws.

The COVID-19 pandemic placed Congress in a similar position. Congress must determine whether it is politically pragmatic to reduce privacy protections to ensure that all Americans are safe from the virus. The key difference between COVID-19 and September 11 is the current sentiment Americans have about personal data privacy.[250]

After September 11, most Americans supported policies ensuring their protection from future terrorist attacks at the expense of privacy.[251] Today, however, most Americans value their privacy over governmental protection from the virus.[252] As a result, Congress must prioritize Americans' privacy while promoting a national campaign that emphasizes transparency and effective communication with the public.

Congress must work to educate the American public on how personal data is being collected and processed. Far too many Americans are unknowledgeable about how companies and other entities collect their personal information.[253] While private organizations, such as nonprofits, might be a workable solution, revamping and expanding federally funded programs devoted to educating Americans about data privacy would assure Americans the federal government understands the issues and will safely regulate private data.[254] If Americans associate data privacy awareness and education with the federal government, members of Congress will be more likely to receive public support to pass a federal data privacy law.

Congress must also assure Americans that their data will be safe from unconsented or unlawful uses. The simplest way to achieve this goal is to utilize the privacy protection clauses in the GDPR and newly enacted CPRA as baseline models. Both laws aim to protect data privacy, and their provisions are familiar to most companies that collect, store, and process personal information.[255]

---

247. *See* Shiva Manium, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RSCH. CTR. (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ [http://perma.cc/YEY2-CZPQ] [hereinafter *Tensions Between Privacy and Security Concerns*].

248. *Id.*

249. *See id.*; *The Cost of Privacy*, *supra* note 183.

250. *See Tensions Between Privacy and Security Concerns*, *supra* note 247.

251. *Id.*

252. *The Cost of Privacy*, *supra* note 183 (explaining that eighty-four percent of Americans worry that they will be giving up too much of their privacy as a result of COVID-19).

253. *See id.*

254. According to the FTC, the Commission provides a range of educational materials to provide guidance to consumers and businesses. *See Privacy & Data Security Update: 2019*, FED. TRADE COMM'N, http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf [http://perma.cc/579C-YP9X] (last visited May 1, 2022). However, a more publicized effort to integrate these programs into local communities is needed.

255. *See* DATAGUIDANCE, *supra* note 18, at 5; Levenberg & Pittman, *supra* note 93.

One limitation of the CPRA and GDPR, however, is their lack of opt-in clauses.[256] Under both laws, when most individuals enter a website, their personal information is collected by default unless they affirmatively opt out.[257] For Americans who do not understand how their data is being collected and processed, the opt-out clause is an inadequate remedy. Instead, Congress should provide additional privacy protections by considering a more expansive opt-in clause. Under an opt-in right, an individual's personal data would not be collected unless they choose to opt in.[258] Ultimately, an opt-in clause would protect a wider spectrum of Americans from unauthorized uses of their personal data.

Finally, Congress will need to consider how future technological advancements will impact Americans' attitudes toward privacy. Over the past ten years, the scale and scope of technology have changed dramatically.[259] Smartphones have become part of everyday life for most Americans, providing widespread access to the digital economy while exposing an increased volume of personal data to collection.[260] Technological innovation continues today with the emergence of drones, smart artificial intelligence devices, and facial recognition software.[261] To enact and enforce the law effectively, Congress must anticipate technological instrumentalities that will be used to collect personal information from unsuspecting Americans. If the law fails to anticipate future data privacy concerns, it would leave Americans without statutory or private recourse to unconsented and unlawful uses of their personal data.

B. Limit the Burden on Companies Collecting Personal Data

When drafting data privacy legislation, Congress must consider excessive compliance and liability costs for covered companies. As evidenced by the enactment of the CCPA in California and SB-220 in Nevada, data privacy regulation inevitably raises compliance costs for companies covered under both laws.[262] While the enactment of a federal data privacy law will bring long-term savings to most companies compared to a state-by-state approach, such savings could be negated if the federal law's scope of protections is too broad or complex. In particular, smaller companies with limited compliance budgets will find it difficult to comply with a set of laws requiring a complete redesign of how companies collect, process, and store personal data.[263] Thus, while

256. *See* Levenberg & Pittman, *supra* note 93.

257. *See id.*

258. Lauren Kaufman, *To Opt-In or Opt-Out*?, MEDIUM (Mar. 6, 2020), http://medium.com/popular-privacy/to-opt-in-or-opt-out-5f14a10bae24 [http://perma.cc/ZXM9-A624].

259. *See* Pedro Palandrani & Andrew Little, *A Decade of Change: How Tech Evolved in the 2010s and What's in Store for the 2020s*, GLOBAL X (Feb. 10, 2020), http://www.globalxetfs.com/a-decade-of-change-how-tech-evolved-in-the-2010s-and-whats-in-store-for-the-2020s/ [http://perma.cc/KK49-JMKB].

260. *See id.*

261. *See id.*

262. *See* Beckerman, *supra* note 9.

263. *See* Paula Bruening, *Crafting a Federal Privacy Law To Benefit Small Businesses*, BLOOMBERG L. (Oct. 5, 2020, 4:01 AM), http://news.bloomberglaw.com/privacy-and-data-security/crafting-a-federal-privacy-law-to-benefit-small-businesses [http://perma.cc/9ZEX-AM4M].

Congress should prioritize providing enhanced data privacy protection, the scope of any proposal should stay reasonably within existing data privacy laws, such as the CCPA, CPRA, and GDPR. By ensuring some legislative predictability, Congress will shield many companies from excess compliance and violation costs.

Additionally, companies would prefer legislation that either limits or eliminates a private right of action.[264] A federal law permitting civil lawsuits against noncompliant companies will not only risk opening the "floodgates of litigation" but also disproportionately harm smaller companies without the capital to employ a full-service compliance team.[265] While protecting privacy rights is essential, Congress cannot ignore the significant costs incurred on the entities it seeks to regulate.

Along with corporate concerns of scope and a private right of action, companies must deal with novel privacy concerns arising as a result of the COVID-19 pandemic. The shift in consumer preferences has increased the volume of personal data companies collect.[266] COVID-19 increased the risk of cyberattacks on company databases, threatening both consumer and employee personal information.[267] Finally, many companies face challenges in managing the collection of health data as employees begin to return to the office.[268]

COVID-19 raised awareness of how health crises can expose data privacy vulnerabilities. Congress should address these pandemic-specific challenges now. However, Congress should also structure legislation to protect personal data when the next major health crisis arrives. Its efforts to pass the CCDPA and PHEPA fall embarrassingly short, focusing solely on healthcare data while leaving a vast majority of other personal information subject to state laws.[269] For companies covered under this legislation, the CCDPA and the PHEPA will only complicate the data privacy regulatory environment. Not only will companies have to comply with a fragmented system of state data privacy laws but they must also determine whether the federal COVID-19 bills preempt each state law.[270] While Congress's intent to pass COVID-19 data privacy legislation is well-intentioned, the CCDPA and the PHEPA are merely patchwork fixes that fail to address broader data privacy issues.

Congress must ensure future data privacy regulations will not be a financial detriment to companies by anticipating a permanent expansion of the digital economy

---

264. *See* John Hendel & Cristiano Lima, *Lawmakers Wrangle Over Consumer Lawsuits as Privacy Talks Drag*, POLITICO (June 5, 2019, 11:04 AM), http://www.politico.com/story/2019/06/05/privacy-advocates-consumer-lawsuits-1478824 [http://perma.cc/WVC8-6R5D].

265. *See id.*

266. *See* Baig, *supra* note 1.

267. Brown & Sood, *supra* note 198.

268. *See* Zoe Argento, Philip Gordon, Kwabena Appenteng & Anna Park, *With COVID-19 Resurgent, Employers Confront Privacy and Information Security Issues When Testing Employees for COVID-19*, LITTLER (Aug. 3, 2020), http://www.littler.com/publication-press/publication/covid-19-resurgent-employers-confront-privacy-and-information-security [http://perma.cc/3LDG-9FKU].

269. *See* Nguyen, *supra* note 185.

270. *See* JONATHAN M. GAFFNEY, ERIC N. HOLMES & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R46542, DIGITAL CONTACT TRACING AND DATA PROTECTION LAW 40 (2020), http://fas.org/sgp/crs/misc/R46542.pdf [http://perma.cc/BS45-MQYD].

and increased work-from-home employees. Existing data privacy bills proposed by Congress have not considered the unique concerns brought about by the pandemic.[271] They also fail to address the risk that smaller businesses will be disproportionately impacted by statutory violations and private rights of action.[272] Ultimately, forward-looking legislation is necessary to keep pace with the rapidly changing state of the American economy and society.

C. Solve the Preemption and Private Right of Action Congressional Deadlock

While focusing on high-level policy objectives will drive congressional action to introduce data privacy legislation, Democrats and Republicans must reach an agreement over the scope of preemption and the inclusion of a private right of action to ultimately enact a data privacy law.[273] Prior congressional data privacy proposals, both pre– and post–COVID-19, have provided similar protections for American consumers, such as a right to opt out and a right to deletion.[274] However, a congressional deadlock over the scope of federal preemption and the inclusion of a private right of action for U.S. citizens hinders further legislative progress.[275]

Part III.C.1 argues that while federal preemption of fragmented state data privacy laws is essential, states should still be permitted to pass broader data privacy laws addressing novel privacy issues. This preemption "compromise" would satisfy Republicans' preference for broad preemption in the short term while accommodating Democrats' preference for state legislative flexibility in the long term. Part III.C.2 argues for a minimal private right of action. While Americans' right to sue companies civilly for data privacy violations would be a significant deterrent, this right could expose companies to frivolous litigation and excessive damages. For Congress to balance these interests, it must require a substantial burden of proof from the plaintiff while also imposing limited damages on the company causing the harm.

1. Preemption Solution

For Congress to pass a federal data privacy law, it must take into account the scope of federal preemption. As of 2021, only three states have enacted data privacy legislation, with California's CCPA being the most influential and comprehensive.[276] Many states have followed California's lead, drafting unique data privacy bills.[277] While not all proposed bills will pass, it is likely a few will become law over the next couple of years.[278]

---

271. Adam Schwartz, *Two Federal COVID-19 Privacy Bills: A Good Start and a Misstep*, ELEC. FRONTIER FOUND. (May 28, 2020), http://www.eff.org/deeplinks/2020/05/two-federal-covid-19-privacy-bills-good-start-and-misstep [http://perma.cc/D6J7-YVGZ].

272. *See* Bruening, *supra* note 263.

273. *See* GAFFNEY, *supra* note 8, at 1.

274. *See id.* at 2–3.

275. *See id.* at 1.

276. *See State Privacy Law Comparison*, *supra* note 5.

277. *See id.*

278. Tabatabai et al., *supra* note 104.

A congressional preemption compromise would eliminate repetitive state laws while also providing future flexibility to state legislatures. A federal law that, at first, expressly preempts state data privacy regulations would have short-term benefits for both companies and citizens.[279] Preempting a fragmented system of state laws would impose uniform regulations on companies, providing significant compliance cost savings.[280] It would also equally protect all Americans' privacy, regardless of the state in which they reside.[281]

While a policy of express federal preemption has significant support from congressional Republicans, Democratic critics of the policy believe express preemption would prevent state legislatures from enacting additional data privacy protections preferred by their constituents.[282] Historically, opponents of express preemption discuss the importance of states as "laboratories" for innovative regulations that Congress fails to address.[283] For data privacy regulations, the effectiveness of privacy protections depends on how personal data is being used and collected. As newer technologies become more commonplace in society, novel data privacy concerns associated with these newer technologies have the potential to surpass protections imposed by a federal data privacy law. Thus, proponents of a narrower preemption policy believe that state legislatures should have the power to impose stricter data privacy regulations when the federal government fails to foresee and quickly act to address particular data privacy issues.[284]

A solution to resolve the congressional deadlock emphasizes the importance of express preemption but also acknowledges the necessity to rapidly address unprecedented data privacy issues in the future. First, a provision that expressly preempts state data privacy laws is required. A federal law that initially provides states with the ability to supplement the legislation will only lead to the same patchwork of laws companies currently have to contend with.[285] However, to achieve bipartisan support in Congress, the law's substantive statutory protections must exceed the scope of the CCPA (and CPRA).[286] While the CCPA is a model statute for many state legislatures seeking to enact data privacy laws, a federal data privacy law must anticipate potential privacy issues that states would independently address.

Second, while the federal law should expressly preempt state laws initially, states should be allowed, after a certain period, to enact broader privacy regulations addressing novel data privacy issues. While encouraging state action could undermine the regulatory regime in place, Congress could still pass additional legislation to expand protections nationally. Thus, if a majority of states begin enacting additional regulations—fulfilling their role as policy "laboratories"—Congress can preempt states by amending the existing law appropriately.

279. *See* Adams, *supra* note 149, at 1092–94.

280. *See id.*

281. *See id.*

282. *See* Kerry & Morris, *supra* note 140.

283. *See* Adams, *supra* note 149, at 1092–94.

284. *See* Kerry & Morris, *supra* note 140.

285. *See id.*

286. *See id.*

2. Private Right of Action

Whether a data privacy law should include a private right of action is another point of disagreement in Congress. Republicans strictly oppose providing a private right of action, while Democrats support a limited private right of action for Americans harmed by a company's statutory violation.[287] This partisan polarization has stalled any progress toward finding a common solution for implementing a private right of action.[288]

The primary concern voiced by critics of the private right of action is a rise in frivolous class action lawsuits leading to excessive damages resulting from settlements.[289] This concern must be taken into consideration when determining how inclusive the private right of action should be. Alternatively, proponents of the private right of action believe it is necessary to provide redress for violations of legally protected privacy interests.[290] In addition, allowing individuals to sue companies for violations serves as another method of enforcement and encourages companies to comply with the regulations.[291]

In terms of existing law, both the CCPA and the GDPR contain provisions providing a private right of action against covered companies.[292] The CCPA limits a private cause of action to incidents involving unauthorized access of unencrypted or nonredacted personal information.[293] Furthermore, the CCPA limits the total recovery per claim.[294] Conversely, the GDPR does not limit the specific cause of action and provides more lenient limits on recovery.[295] Democratic legislators in favor of the private right of action acknowledge that the GDPR provision is too broad to be implemented effectively in the United States.[296]

One serious issue with the CCPA's private right of action provision is its "per incident" recovery structure. Under the CCPA, companies can be sued for no more than $750 per incident or actual damages, whichever is greater.[297] While this seems like a reasonable limit on litigation costs, larger class action suits could amass significant potential damages, incentivizing companies to settle even frivolous claims.[298] These claims can be particularly damaging to smaller businesses that are covered under the

287. *See* Feiner, *supra* note 155.

288. *See id.*

289. Kerry & Morris, *supra* note 161.

290. *Id.*

291. *Id.*

292. DATAGUIDANCE, *supra* note 18, at 39.

293. *Id.*

294. California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.150(a)(1)(A) (West 2021).

295. DATAGUIDANCE, *supra* note 18, at 39–40.

296. This viewpoint is evidenced by Democratic-sponsored bills, which place similar limits to the private right of action as the CCPA. *See* GAFFNEY, *supra* note 8, at 1.

297. *See* CAL. CIV. CODE § 1798.150(a)(1)(A).

298. *See* Elizabeth Snyder, *Potentially Expanded Private Right of Action Increases Risk of Class Action Exposure Under the California Consumer Privacy Act*, DORSEY & WHITNEY LLP (May 1, 2019), http://www.dorsey.com/newsresources/publications/client-alerts/2019/04/private-right-of-action-increases-risk [http://perma.cc/6EWA-MDC9].

law.[299] Thus, under a federal framework, Congress should prioritize these risks while drafting a private right of action provision.

While Republicans and corporations are generally opposed to allowing individuals to file civil lawsuits under data privacy legislation, America's privacy landscape includes many laws that contain private rights of action.[300] One example is the Telephone Consumer Protection Act, which has produced massive damages awards for class action claims.[301] The Telephone Consumer Protection Act, which regulates robocalls, allows a strict liability private right of action for each violation up to $500.[302] This unlimited "per incident" approach has led to crippling private action claims.[303] A private right of action is appropriate when reasonable limits are imposed on damages and particular claims. Providing Americans with redress for actual harm caused by statutory violations of a data privacy law is appropriate and necessary. However, without reasonable limits, companies risk being disproportionately impacted by meritless class action claims filed by opportunistic plaintiffs' attorneys.

For Congress to find an appropriate balance, it needs to impose specific barriers to filing a claim. First, to ensure constitutional standing under *Spokeo*, Congress must limit the claims' scope to actual harm.[304] Next, Congress should specify that only certain types of harm are recoverable. Since most companies have structured their compliance departments around the CCPA's enforcement policies,[305] Congress should provide similar limits to types of harm in its initial proposal. Finally, Congress should place a ceiling on the amount of recoverable damages for class action suits. Since the "per incident" limit could be abused through frivolous class action lawsuits,[306] placing a ceiling on the total damages per individual would provide reasonable limits to massive class action claims.

D. Address COVID-19–Related Data Privacy Concerns

The impact of the COVID-19 pandemic on cybersecurity and healthcare data created additional issues for Congress to address when considering a federal data privacy law.[307] Congress recognized healthcare data privacy concerns when it proposed the CCDPA and PHEPA to provide oversight for employers collecting employee healthcare

299. *See id.*

300. *See* Kerry & Morris, *supra* note 161.

301. *Id.*

302. *Id.*

303. *See* Charles Insler, *Who's Calling? TCPA Litigation in the Aftermath of* Spokeo, ABA (Feb. 16, 2017), http://www.americanbar.org/groups/business_law/publications/blt/2017/02/06_insler/ [http://perma.cc/NST4-Y74Z].

304. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (holding that a plaintiff must show an invasion of a legally protected interest that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical").

305. *See* Greg Bensinger, *So Far, Under California's New Privacy Law, Firms Are Disclosing Too Little Data – or Far Too Much*, WASH. POST (Jan. 21, 2020), http://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/ [http://perma.cc/T84Y-99K5].

306. *See Understanding the Telephone Consumer Protection Act*, GREENBERG TRAURIG (Apr. 9, 2020), http://www.gtlaw.com/en/insights/2020/4/understanding-the-telephone-consumer-protection-act [http://perma.cc/AZW5-KREB].

307. *See* Brown & Sood, *supra* note 198.

data for tracking purposes.[308] However, these bills are narrowly construed and fail to address the issue of an inadequate system of fragmented state privacy bills. In addition, Congress has not directly addressed the concerns of an increased cybersecurity threat that implicates healthcare providers and other organizations that collect, store, and process sensitive information. Part D.1 discusses why the provisions in the CCDPA and PHEPA should be included in a federal data privacy law. Part D.2 discusses the necessity for Congress to provide protections to companies from increased cybersecurity threats.

1. Integrate Existing COVID-19 Healthcare Data Bills

The COVID-19 pandemic altered the way employers and companies collect, store, and process healthcare information. Since COVID-19 has magnified healthcare data privacy issues, Congress must attempt to integrate a broad healthcare data privacy mandate. Congress can achieve this by incorporating parts of the CCDPA and PHEPA into a federal data privacy bill. While the CCDPA primarily regulates the private sector's contact tracing efforts,[309] the PHEPA provides a broader mandate regulating government-based tracing of emergency health data and banning third-party sales of emergency health data.[310]

Under a PHEPA-like provision, companies could still collect sensitive healthcare information. This broader mandate to protect sensitive healthcare data could create mistrust among American consumers that their data is used to determine eligibility for future employment and access to healthcare.[311] However, the law would merely ensure that companies securely store sensitive healthcare information and enforce that this information is not sold on the secondary market.

While the integration of PHEPA provisions would protect American consumers' sensitive healthcare data, it would not direct employers on how they should collect, store, and process sensitive employee healthcare data. Currently, the EEOC serves as the federal agency that directs employers on these matters and has provided detailed guidance on how to safely store healthcare data during the pandemic.[312] However, the EEOC has not yet anticipated how this data will be treated once the pandemic ends.[313] This gap in regulatory coverage provides Congress an opportunity to provide additional oversight for employee healthcare data.

As of 2020, both Republicans and Democrats prefer the FTC as data privacy law's primary enforcement agency.[314] However, for employment-related regulations, the EEOC might be more effective in enforcing the law.[315] In this light, Congress should

308. *See* Nguyen, *supra* note 185.

309. *See id.*

310. *See id.*

311. AM. BAR ASS'N: ANTITRUST L. SEC, PRESIDENTIAL TRANSITION REPORT: THE STATE OF ANTITRUST ENFORCEMENT 52 (2021), http://www.americanbar.org/content/dam/aba/administrative/antitrust_law/lp-files/presidential-transition-report.pdf [http://perma.cc/W6PZ-SGB4].

312. *See* EEOC, *Pandemic Preparedness*, *supra* note 201.

313. *See id.*

314. Davis, *supra* note 139.

315. The purpose of the EEOC is to "[e]nforc[e] federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex . . . national origin,

carve out an exception that directs the EEOC to enforce any federal provisions in the law that relate to employment healthcare data privacy. Under this structure, Congress can append an employment healthcare data provision that would provide a long-term solution to protect the privacy of employees' healthcare data.

2. Protect Cybersecurity Threats

Another data privacy risk caused by the COVID-19 pandemic is an increased number of cyberthreats and cyberattacks on U.S. companies.[316] In particular, cybercriminals are likely to target remote workers to attempt to hack into company databases.[317] In addition, there are concerns that cybercriminals will target institutions that collect or store sensitive information, including hospital systems and government agencies.[318] While a few government agencies have issued cybersecurity warnings to businesses and individuals working from home, no substantive legislative action has addressed this concern.[319]

While regulating cyberthreats falls outside the scope of a federal data privacy law, Congress can act as a safeguard for companies that are at risk of cyberattacks and data breaches. Congress can appropriate federal funding to directly support or subsidize cybersecurity protections for U.S. companies. The funding would allow companies to either purchase or upgrade their current cybersecurity measures. Additional federal funding could also be allocated to cybersecurity firms to support innovation efforts and strengthen the private sectors' efforts to prevent cyberattacks.

In such a law, Congress should include an exculpation provision to protect companies that suffer cybersecurity attacks but have made good faith efforts to address cybersecurity concerns since the pandemic. The immunity offered by the exculpation clause would allow firms that act in good faith to rebuild their infrastructures without the added costs of governmental fines or private class action litigation. While an exculpation clause could be underinclusive, imposing significant fines and damages on firms that have taken action to protect their cybersecurity systems would be counterproductive by disincentivizing firms to make necessary upgrades to their information technology systems.

IV. CONCLUSION

The COVID-19 pandemic has had a striking effect on the U.S. economy.[320] As more Americans begin to regularly engage in the digital economy, the federal government has a duty to regulate how companies should properly collect, process, and store personal data. Data privacy regulations must anticipate how COVID-19 implicated employee data privacy and novel cybersecurity attacks.[321] While Congress intended to pass a federal

age, . . . disability or genetic information." *Overview*, EEOC, http://www.eeoc.gov/overview [http://perma.cc/VFN9-AML2] (last visited May 1, 2022).

316. Brown & Sood, *supra* note 198.

317. *See id.*

318. *See id.*

319. *See Managing Cybersecurity*, *supra* note 3.

320. *See supra* notes 187–195 and accompanying text.

321. *See supra* notes 198–200 and accompanying text.

data privacy law in response to COVID-19, it failed to do so.[322] Instead, many states are taking action, potentially creating a patchwork of data privacy laws that not only straps companies with significant compliance costs but also creates inequalities between citizens of neighboring states.[323] While some states, like California and New York, propose sweeping legislation to broadly protect personal data, others do not.[324] The economic and societal challenges brought by COVID-19 should be a wake-up call to Congress: pass a federal data privacy law or risk the high political cost of inaction.

322. *See supra* Part II.C.

323. *See supra* notes 101–135 and accompanying text.

324. *See supra* Part II.B.