Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 16
Issue 1 *SYMPOSIUM A Life Navigating the Securities Markets: A Celebration of Professor Roberta Karmel's Work, Teaching, and Mentorship*

Article 15

12-1-2021

Revising U.S. Privacy Laws: New Laws are Required to Fill in the Gaps of Current and Proposed Legislation to Account for New Technologies and Future Emergencies

Marissa Wong

REVISING U.S. PRIVACY LAWS: NEW LAWS ARE REQUIRED TO FILL IN THE GAPS OF CURRENT AND PROPOSED LEGISLATION TO ACCOUNT FOR NEW TECHNOLOGY AND FUTURE EMERGENCIES

ABSTRACT

With the ongoing expansion of internet services and increase in cyberattacks, Congress has long recognized the need for comprehensive federal privacy legislation, but no federal legislation has been passed. Currently, the scatter-shot of sector and state-specific privacy laws have proven to be ineffective. The authority of the Federal Trade Commission (FTC) has also been weak. The unexpected occurrence of the COVID-19 pandemic further exposed the dire need for comprehensive federal privacy legislation. Data-collection methods such as facial recognition, immunity passports, and contact tracing leave users' health and location data vulnerable in the hands of the government and private companies. Technologies such as Zoom have also revealed privacy concerns. Amongst the many state-based privacy laws, the California Consumer Privacy Act (CCPA) is the most comprehensive state law to date. It governs every company that does business with a California company, has California resident customers, or collects any personal data of a California resident. However, this Note will suggest that the CCPA and other state and sector-based regulations still leave loopholes. While there are comprehensive federal privacy bills being proposed, none have been passed due to the inability of the political parties to agree on the issues of preemption and private right of action. This Note will suggest a new approach to federal privacy regulation – a revised private right of action component, a sunset provision for preemption, and a minimization of disparate impact and increased scope of governance in COVID-19-responsive legislation.

INTRODUCTION

> "If you are not paying for it, you're not the customer; you're the product being sold."[1]

An average American's information can be found in anywhere between twenty-five and one hundred commercial databases.[2] Some data collection companies make their money solely by selling information about consumers to employers, marketers, and others.[3] Consumers contribute to the data in

1. Will Oremus, *Are You Really the Product*, SLATE (Apr. 27, 2018), https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html/.

2. Tanith L. Balaban, Note, *Comprehensive Data Privacy Legislation: Why Now Is the Time?,* 1 CASE W. RSRV. J. L. TECH. & INTERNET 1, 5 (2009).

3. *Id.*

these systems when they conduct a Google search, purchase something online, or create a Facebook profile.[4] Personal information has been turned into commodities with the opportunity for data abuse.[5] Naturally, data privacy has been a debated issue.[6]

Current and proposed data privacy legislations require re-examination. Rather than unrealistically expecting consumers to protect their own privacies, a federal privacy framework needs to be solidified to protect consumers.[7] The stakes are high when it comes to privacy. On July 19, 2020, Judge Salas's family was targeted due to her position as a woman on the bench.[8] Lack of privacy allowed the murderer to kill her son after accessing her family's address and other personal information.[9] In an effort to push for privacy protection, Judge Salas said:

> In my case, the monster knew where I lived and what church we attended and had a complete dossier on me and my family. At the moment, there is nothing we can do to stop it, and that is unacceptable. My son's death cannot be in vain, which is why I am begging those in power to do something to help my brothers and sisters on the bench.[10]

Later, "Daniel's Law," a privacy bill named after Judge Salas' son, was passed to prohibit the posting of home addresses and phone numbers of judges, prosecutors, and law enforcement.[11] Similar privacy protections need to be extended to consumers through federal privacy legislation.

If Judge Salas' situation is not convincing enough, the concerns surrounding Facebook will hopefully put the cherry on top. On October 5th, 2021, Frances Haugen, a previous Facebook employee and now whistleblower, testified before a Congressional Subcommittee the harms perpetuated by Facebook.[12] Haugen testified that Facebook's internal research showed that its use of its algorithm, that was derived from users' private data to target users with relevant content, was negatively impacting

4. *Id.*

5. *Id.*

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

7. *Id.*

8. David Wildstein, *After Murder of Federal Judge's Son, Assembly Passes Bill to Protect Privacy of Judges, Prosecutors, Law Enforcement*, N.J. GLOBE (Sept. 24, 2020), https://newjerseyglobe.com/legislature/after-murder-of-judges-son-assembly-passes-bill-to-protect-privacy-of-judges-prosecutors-law-enforcement/.

9. *Id.*

10. Eric Levenson, *New Jersey Federal Judge Whose Son Was Killed Details His Last Words*, CNN (Aug. 3, 2020), https://www.cnn.com/2020/08/03/us/federal-judge-esther-salas/index.html.

11. Wildstein, *supra* note 8.

12. Rachel Popa & Chandler Ford, *Privacy Implications of the Facebook Whistleblower Testimony*, NAT'L L. REV. (Oct. 15, 2021), https://www.natlawreview.com/article/privacy-implications-facebook-whistleblower-testimony.

teens' mental health.[13] She further testified that the tech giant puts profits over its users' safety, favoring growth over moderating harmful content.[14] The heart of the problem relates to user data privacy – Facebook chose to capitalize on users' data, targeted their insecurities by using their data, and continues to generate profit off this.[15] As a result, lawmakers are discussing possible new national privacy legislation through child safeguard laws.[16]

Comprehensive federal privacy law is necessary to cease confusion from the scattershot of sector and state-based laws, and to effectively protect data as technology continues to develop and remain boundless. Congress needs to enact legislation that preempts state laws, provides redress, protects health data during public health emergencies, and minimizes disparate impact.

In Part I, this Note will discuss the background and current state of privacy laws in the U.S. Part II will examine the current regulation and enforcement efforts. Then, Part III will discuss privacy issues posed by COVID-19 mitigation efforts. Next, Part IV will discuss the most recently proposed laws. Part V will examine why the current and proposed laws are insufficient for the future of privacy in the U.S. Lastly, Part VI will propose a solution requiring preemption of state laws, redress for victims, protection over health data collected through mitigation technologies and efforts, and minimization of disparate impact.

I. BACKGROUND: THE CURRENT STATE OF U.S. PRIVACY LAW

The U.S. has favored sector-specific and state-based legislation.[17] The rise of the Internet, which knows no borders, has led to the increased need for new privacy laws.[18] Privacy issues are further magnified as data privacy concerns are raised through COVID-19 pandemic mitigation efforts.[19]

A. SECTOR AND STATE SPECIFIC PRIVACY LEGISLATION

First, sector-specific legislation has led to user privacy complications.[20] One example of sector-specific legislation is the Health Insurance Portability and Accountability Act (HIPAA) which governs personal health information.[21] While HIPAA is a federal law that protects individuals' health information, it only applies to certain healthcare entities, such as a doctor's

13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. *Is a Federal U.S. Data Protection Regime Closer Than We Thought?*, LEXOLOGY (June 30, 2020), https://www.lexology.com/library/detail.aspx?g=21821e38-0a05-4ca5-8d69-3ba2a34ab6f1.
18. *Id.*
19. *Id.*
20. *See id.*
21. *Id.*

office, and generally does not cover data provided by consumers through other methods such as fitness apps or devices.[22] Sector-specific legislation like HIPAA leaves loopholes and defers to states to fill in its gaps.[23]

State-specific privacy laws, the second type of non-federal privacy legislation, have also been ineffective in a comprehensive unified sense.[24] Different privacy laws in different states lead to confusion for consumers and businesses.[25] For example, the technology industry, a sector guided by state-specific laws, has historically been lightly regulated.[26] Undeniably, consumers may not have a problem with Netflix suggesting recommendations to them based on their viewing history.[27] However, the problem with big tech companies collecting data from consumers is that the data often leaves the companies' hands and control.[28] Aside from the dangers of individual data breaches, platforms such as Facebook already have full permission to sell and manage consumer data. [29] One example is the Cambridge Analytica Scandal that involved Donald Trump's political consulting firm's work on his 2016 presidential campaign.[30] The firm created surveys that several hundred thousand Facebook users completed and the survey required users to download a Facebook application (app) named "This is Your Digital Life."[31] Unknowingly, the app allowed the firm to collect personal information of the users and all of their Facebook friends.[32] This resulted in the harvesting of over fifty million Facebook users' personal data for the purpose of creating "psychographic profiles" of voters in advance of the 2016 election.[33] Even after Facebook learned of the data breach, it never bothered to alert its users.[34]

Americans were troubled by Facebook's access to their data, and consumers were left wondering what else Facebook and other tech companies have access to.[35] Facebook and other tech giants' terms of services are often complex and consumers do not bother to read the lengthy agreements.[36] This

22. Caitlin Wilmot, *Everyone Agrees – We Need a Comprehensive U.S. Privacy Law*, JD SUPRA (Sept. 26, 2020), https://www.jdsupra.com/legalnews/everyone-agrees-we-need-a-comprehensive-85012/.

23. *See id.*

24. *See id.*

25. *Id.*

26. Daniel Kelly, *Is It Time for New U.S. Data Privacy Laws?*, WEXLER WALLACE (May 1, 2019), https://www.wexlerwallace.com/time-new-data-privacy-laws/.

27. *Id.*

28. *Id*

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. *See* Chloe Aiello, *Senator to Zuckerberg: 'Your user agreement sucks'*, CNBC (Apr. 10, 2018), https://www.cnbc.com/2018/04/10/senator-to-zuckerberg-your-user-agreement-sucks.html.

is reflected in Senator John Kennedy's statement to Facebook's Chief Executive Officer Mark Zuckerberg: "[Y]our user agreement sucks…[T]he purpose of a user agreement is to cover Facebook's rear end, not inform users of their rights."[37] While consumers rarely read the lengthy terms of service agreements, it would not make a difference if they did since consumers often have no option but to agree to the terms if they want to use the service.[38]

These issues raise genuine concern and has caused some states to enact their own privacy laws.[39] A patchwork of fifty sets of laws would confuse businesses and consumers, and hit small businesses and small government agencies heavily.[40] Comprehensive federal privacy laws would unify data protection enforcement, make application of privacy law more consistent, and relieve the burden of trying to ensure compliance with not just multiple state laws, but across different sectors.[41] State-by-state privacy laws would mean that a woman from California who orders an item from a Missouri business that manufactures in Florida could have her data regulated by three separate state laws, or by no laws, depending on the state.[42] While California has promulgated its own privacy law, its residents still cannot be assured that the protections apply when they deal with a party not covered by the law.[43] This patchwork of laws leads to inconsistent treatment of data depending on factors such as the residency of the consumer.[44] As a result, consumers cannot be confident that their data will remain protected from state to state.[45]

B. STATES: CALIFORNIA'S DATA PRIVACY LEGISLATION

The most comprehensive state data privacy legislation to date is the California Consumer Privacy Act (CCPA), which went into effect in January 2020.[46] The CCPA applies to for-profit businesses that (1) have an annual gross revenue of at least $25 million, (2) buy, receive, sell, or share consumer data from 50,000 or more consumer households, or devices, or (3) gain a

37. *Id.*

38. David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, THE GUARDIAN (Mar. 3, 2017), https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print.

39. Casey Stanley, *Why the Country Needs a National Data Privacy Framework*, GOV'T TECH. (Oct. 1, 2019), https://www.govtech.com/opinion/Why-the-Country-Needs-a-National-Data-Privacy-Framework-Contributed.html.

40. *Id.*

41. LEXOLOGY, *supra* note 17.

42. Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html.

43. *Id.*

44. *Id.*

45. *Id.*

46. Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), https://www.osano.com/articles/data-privacy-laws.

majority of their annual revenue from the selling of personal data.[47] The Act governs beyond California residents; it applies to every company that does business with a California company, has California resident customers, or collects any personal data of a California resident for any purpose.[48] The goal of the CCPA is to give California residents more control over their personal data that companies collect and process.[49] According to Berkeley Economic Advising and Research, LLC's Standardized Regulatory Impact Assessment, the CCPA regulation will protect over $12 billion worth of personal information used for advertising each year in California.[50]

The CCPA secures new privacy rights for California consumers such as the right to know about the personal information a business collects about them and how it is used and shared, the right to delete personal information collected from them, the right to opt-out of the sale of their personal information, and the right to non-discrimination for exercising their CCPA rights.[51] The consumers can request for businesses to disclose to them what personal information they have collected, used, shared, or sold about them and why they collected, used, shared, or sold that information.[52] This also applies to the categories of third parties with whom the business shares the personal information.[53]

The CCPA left some loopholes that were exploited by some big tech companies.[54] For instance, tech companies capitalized on the opportunity to exempt themselves from: (1) the CCPA's provision that allows users to opt-out of the "sale" of their data and (2) the CCPA's provision that allowed service providers who need data to perform a "business purpose."[55] Big tech companies argue that they do not sell data; they simply share it.[56] As a result, consumers cannot opt-out since they are not "selling" data.[57] Additionally, companies claim that they are acting pursuant to a "business purpose" of providing targeted advertising.[58] As a result, companies would be exempt

47. Tom Kulik, *Some Big Reasons Why the CCPA Is More of A Problem Than You Think*, ABOVE THE LAW (Oct. 28, 2019), https://abovethelaw.com/2019/10/some-big-reasons-why-the-ccpa-is-more-of-a-problem-than-you-think/.

48. Arlo Gilbert, *California Consumer Privacy Act (CCPA) Compliance Guide: Everything You Need to Know*, OSANO (Aug. 19, 2021), https://www.osano.com/articles/ccpa-guide.

49. Yunge Li, *The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth?*, 32 LOY. CONSUMER L. REV. 177, 180 (2019).

50. Gilbert, *supra* note 48.

51. *California Consumer Privacy Act (CCPA)*, CAL. ATT'Y. GEN., https://oag.ca.gov/privacy/ccpa (last visited Dec. 27, 2020).

52. *Id.*

53. *Id.*

54. Prop 24 Expands Data Privacy Law, BALLOT.FYI (Oct. 26, 2020), https://www.ballot.fyi/prop-24 [hereinafter Prop 24].

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

from the Act.[59] For example, Facebook challenged its obligation to comply with the CCPA's provision by defining itself as a "service provider" who does not directly sell data it collects to third-party companies but only acts as a service that runs advertisements.[60] These loopholes were catalysts in passing of the California Privacy Rights Act (CPRA), effective January 1, 2023, which filled the gaps in the CCPA.[61]

The CPRA expanded the CCPA's applicability to businesses that generate most of their revenue from sharing personal information, not just selling it; it changed the "Do not sell" clause to "Do not sell or share," which clarifies that targeted advertising is not a "business purpose."[62] The CPRA doubled the CCPA's threshold number of consumers or households from 50,000 to 100,000, which reduced its applicability to small and midsize businesses.[63] Another notable expansion is the CPRA's new category of "sensitive personal information," which includes government identifiers such as social security numbers, financial accounts, login information, precise geolocation, race, ethnicity, religious or philosophical beliefs, genetic data, and sexual orientation information.[64] In other words, the CPRA's expansion will affect many more businesses and categories.

C. STATES: OTHER STATES' DATA PRIVACY LAWS

Maine and Nevada also have state-based privacy laws.[65] However, Maine's privacy laws only apply to internet service providers and not to other types of companies that collect consumer data.[66] Maine's laws include the right to restriction of processing information, the right to opt-out of sale of personal data, transparency requirements, and non-discrimination requirements.[67] Similarly, Nevada's laws apply only to website operators and not to businesses that collect data offline.[68] Nevada's law includes the right to restriction of processing, transparency requirements, and data breach notification.[69] Compared to California's broad interpretation of what

59. *Id.*

60. Eric Westerhold, *Facebook's Attempt to Dodge Compliance with CCPA: We Don't Sell Your Data*, GEO. L. TECH. REV. (March 2020), https://georgetownlawtechreview.org/facebooks-attempt-to-dodge-compliance-with-ccpa-we-dont-sell-your-data/GLTR-03-2020/.

61. Prop 24, *supra* note 54.

62. *Id.*

63. Elizabeth Harding & Alex Polishuk, *CPRA – What This Means for Your Business*, JD SUPRA (Nov. 10, 2020), https://www.jdsupra.com/legalnews/cpra-what-this-means-for-your-business-36612/.

64. *Id.*

65. Gabe Turner, *47 States Have Weak or Nonexistent Consumer Data Privacy Laws*, SECURITY.ORG (Apr. 14, 2020), https://www.security.org/resources/digital-privacy-legislation-by-state/.

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

comprises "sale," Nevada's rule is more oriented towards exclusion of things that are not literally the exchange of money for information.[70]

Companies that look to operate between states must navigate between separate laws that regulate the sale of data.[71] For example, companies that want to operate between California and Nevada must abide by laws that differ vastly since both states cannot agree on basic elements of privacy such as when and how a person can opt-out of having his or her data sold.[72] If companies do not have enough information to tell whether someone is a resident of a certain state, they must choose between applying one state's standard to all individuals nationwide or collecting more information about this person's location to make a decision.[73] If two states have differing obligations for companies, the company would need more personal information, which can be contrary to the goal of privacy laws.[74]

Furthermore, state-by-state legislation can put small business owners at a disadvantage because the varying regulatory environment requires experts, lawyers, and other resources that only better-resourced companies have.[75] This can contribute to the U.S. ceding its position as a leader in technology since many start-ups and entrepreneurs will be unable to navigate the complex data laws of every state that they want to do business in.[76] A federal law with consistent standards for online and offline companies regardless of the residency of their customers would be beneficial and prevent any hinderance on the country's position as a leader in technology.[77]

II. STEPS TOWARDS COMPREHENSIVE PRIVACY LEGISLATION

However, a high momentum of privacy legislation has pushed the U.S. to further its efforts to pass comprehensive federal privacy legislation.[78] Only seventeen states have failed to introduce state-level privacy legislation.[79] While not all of the proposed state laws will ultimately be passed, analyzing the key provisions of each bill can be an indicator of how privacy law is trending in the U.S.[80] Compared to the limited implications of Maine's and Nevada's legislation, California, Colorado, and Virginia have passed comprehensive privacy legislation that encompasses both consumer rights

70. *Id.*
71. Beckerman, *supra* note 42.
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. Sarah Rippy, *U.S. State Privacy Legislation Tracker*, IAPP (Sept. 16, 2021), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
79. *Id.*
80. *Id.*

and business obligations.[81] Additionally, Massachusetts, New York, North Carolina, Ohio, and Pennsylvania either introduced legislation or have legislation in committee.[82]

The Colorado Privacy Act (CPA), within the Colorado Consumer Protection Act[83] and effective on July 8, 2021, is similar to the CCPA.[84] However, the CPA applies to entities that conduct business in Colorado, including producing or delivering products or services targeted to Colorado residents.[85] In contrast to the CCPA, the CPA does not have a revenue limit, and as a result, a business cannot be held to the law solely because of its annual revenues.[86] The CPA also omits individuals acting in a "commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."[87]

Furthermore, the CPA defines the "sale" of data similar to the CCPA, which occurs when personal data is exchanged for "other valuable consideration" and is not limited to "monetary consideration."[88] Additionally, the definition of "sale" excludes certain types of disclosures similar to those in the California Data Protection Act (CDPA).[89] These disclosures include "disclosures to a processor that processes the personal data on behalf of a controller, disclosures of personal data to third party for purposes of providing a product or service requested by consumer, disclosures or transfer of personal data to an affiliate of the controller's," and more.[90] The CPA requires entities to exercise certain duties as well. Entities must exercise the duties of transparency and purpose specification, duty of data maximization, duty to avoid secondary use, duty of care, duty to avoid unlawful discrimination, duty regarding sensitive data, and duty to conduct and document data protection assessment.[91]

---

81. *Id.*

82. *See id.* "In committee" refers to a bill that is scheduled for public hearing where its merits and disadvantages are discussed. *See In Committee*, U.S. HOUSE OF REPRESENTATIVES, https://www.house.gov/the-house-explained/the-legislative-process/in-committee (last visited Oct. 9, 2021).

83. *State Laws Related to Digital Privacy,* NAT'L CONF. ST. LEGISLATURES (July 22, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

84. Sarah Rippy, *Colorado Privacy Act Becomes Law*, IAPP (July 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

85. *Id.* (explaining that the CPA applies to an entity that "[c]onducts business in Colorado or produces or delivers commercial products or services that are internationally targeted to residents of Colorado; and controls or processes the personal data of at least 100,000 consumers or more during a calendar year; or derives or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more").

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

91. Shelly Kim, et al., *Colorado Privacy Act: What Businesses Need to Know*, JD SUPRA (July 26, 2021), https://www.jdsupra.com/legalnews/colorado-privacy-act-what-businesses-9756798/.

The duties of transparency and purpose specification require controllers to provide accessible, clear, and meaningful privacy notice to consumers including things such as the categories of personal data collected or processed by the controller or a processor, the purposes for which personal data is processed, and the express purposes for which personal data is processed.[92] The duty of data maximization mandates that "a controller's collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes for which the data is processed."[93] Furthermore, the duty to avoid secondary use requires a controller to not process personal data for purposes "that are not reasonably necessary or compatible with the specified purposes which the personal data are processed, unless the controller first obtains the consumer's consent."[94] The duty of care requires a controller to "take reasonable measures to secure personal data during both storage and use from unauthorized acquisition" and the duty to avoid unlawful discrimination requires that a controller "shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers."[95] The duty regarding sensitive data also states that a controller shall not "process a consumer's sensitive data without first obtaining the consumer's consent."[96] Lastly, the duty to conduct and document data protection assessment requires that a controller "not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired on or after the effective date of this section that present a heightened risk of harm to a consumer."[97]

The Virginia Consumer Protection Act, effective on January 1, 2023, affects persons conducting business in the Commonwealth and who "(1) either control or process personal data of at least 100,000 consumers or (2) derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers."[98] However, the Act does not apply to state or local government.[99] Consumers have access to their personal data and can correct or delete it and opt-out of targeted advertising.

After Virginia and California passed comprehensive privacy legislation, the Information Transparency and Personal Data Control Act was introduced

92. *Id.*
93. *Id.*
94. *Id.*
95. S. B. 21-190, 73rd Gen. Assemb., Reg. Sess. (Col. 2021).
96. *Id.*
97. *Id.*
98. *State Laws Related to Digital Privacy*, *supra* note 78.
99. *Id.*

on a national level.[100] The Act is the first piece of comprehensive privacy legislation introduced in the 117th U.S. Congress by Rep. Suzan DelBene, D-Wash.[101] The significance is that the Act claims to be a middle-ground between Democrats and Republicans as it seeks to attract support and eventual passage.[102] Previous versions of DelBene's federal comprehensive privacy legislation were stalled due to insufficient support from Republicans.[103] It is also uncertain if this Act will be the last and final one.[104]

The Act is more business-friendly than previous bills proposed by Democrats.[105] It does not include a private right of action and exempts small businesses from a bi-yearly privacy audit performed by a "qualified, objective, independent third party."[106] Small businesses are those that "collect, store, process, sell, share, or otherwise use the sensitive personal information of 250,000 people or fewer per year."[107] The Act also includes a preemption provision that would resolve the issues pertaining to the scattershot of privacy laws but "would not affect state laws related to data breaches, biometrics, wiretapping or public records."[108] These provisions are in line with Republican privacy legislation.[109]

Generally, the Act empowers consumers to opt-out of collection, processing and sharing of non-sensitive information, such as public information, by companies at any time and expand the Federal Trade Commission (FTC) rulemaking authority, such as requiring entities to obtain affirmative opt-in consent, to target entities that "collect, transmit, store, process, sell, share or otherwise use the sensitive personal information of members of the public."[110] Sensitive personal information is protected under the Act and includes "financial account numbers and authentication credentials…; health information; genetic data; … social security numbers…; precise geolocation information, the content of oral or electronic communications; biometric data; … citizenship or immigration status; mental or physical health diagnoses, religious beliefs; and web browsing history and application usage history."[111]

Enforcement of the Act will be exercised through the FTC and the state attorney general, and would require the hiring of 500 new FTC employees,

100. Müge Fazlioglu, *The First But Not the Last Comprehensive U.S. Privacy Bill of 2021*, IAPP (Mar. 17, 2021), https://iapp.org/news/a/the-first-but-not-the-last-comprehensive-u-s-federal-privacy-bill-of-2021/.
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*

including 50 who have "technology expertise."[112] Any state's attorney general may bring an action on behalf of the state's resident if the FTC fails to act within a 60-day period after discovering or being on alert of the violation.[113] While it is unclear whether the Act will be passed, the dire need for uniform federal legislation still remains.

A. THE FEDERAL TRADE COMMISSION ("FTC"): POWERS AND LIMITATIONS

The FTC was initially established to ensure fair competition in commerce.[114] Section 5 of the FTC Act gives the agency broad jurisdiction over commercial entities under its authority to prevent "unfair or deceptive acts or practices in or affecting commerce."[115] Due to Congress' urge to govern privacy, the FTC became involved with consumer privacy cases.[116] The FTC served as a backdrop to the self-regulatory regime of companies in order to not stifle the growth of online activity.[117] Under Section 5, the FTC has two bases for finding privacy issues – "deceptive" and "unfair" trade practices.[118] An unfair or deceptive act is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment," or a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[119] Although Section 5 does not grant the FTC specific authority to regulate privacy, it has been construed to prohibit certain privacy invasions based on deception.[120] However, the FTC still faces significant limits in power.[121]

One limitation of the FTC is its inability to issue fines for Section 5 violations since fines can only be issued for violations of consent decrees.[122] Furthermore, certain industries are exempt from FTC Section 5 enforcement.[123] Moreover, private causes of action are not available.[124] While

112. *Id.*
113. *Id.*
114. Federal Trade Commission Act, 15 U.S.C. § 45 (2006).
115. *Id.*
116. Daniel Solove & Woodraw Hartzog, *The FTC And The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598 (2014).
117. *Id.*
118. *Id.* at 599.
119. *Id.*
120. Chris Hoofnagle, Woodrow Hartzog & Daniel Solove, *The FTC Can Rise to the Privacy Challenge, but not without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.
121. *Id.*
122. *Id.*
123. Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards?*, 27 CATH. U. J. L. & TECH. 77, 85 (2018).
124. *Id.*

the FTC has developed accountability standards that lay out best practices for companies using consumer data in their specific industry, these best practices are not mandatory and as a result, companies do not have to oblige by them.[125]

The FTC's "deception authority" is another limitation: if a company makes a promise in its privacy policy and fails to carry that out, the FTC can only act because of the deception.[126] However, if the company does *not* promise to protect privacy, there is not much the agency can do.[127] Moreover, the FTC's jurisdiction is limited since it generally does not have authority over several sectors, including government agencies, non-profits, banks, insurers, and transportation companies.[128] It is impossible for the FTC to act as a comprehensive privacy regulator because of the many areas that fall outside of its authority.[129]

Another limitation is that each action against big companies requires meticulous investigation before the agency can even obtain any relief for consumers.[130] The FTC is severely understaffed in privacy, with only forty full-time staff members as of Spring 2019.[131] This is a very low number compared to countries with smaller populations than the U.S., such as the hundreds of staff members in Britain and almost 150 each in Ireland and Canada.[132]

Lastly, the FTC does not require companies to enact specific practices or privacy policies.[133] The majority of its cases against companies end in settlements or consent decrees.[134] As a result, the FTC is unable to establish a foundation for privacy law.[135] Naturally, companies have resorted to developing their own privacy practices.[136]

III. DATA COLLECTION THROUGH COVID-19 MITIGATION EFFORTS AND ITS DANGERS

COVID-19 mitigation strategies have exacerbated and fast-tracked the need for new privacy laws. For example, PopID, a provider of thermal facial recognition technology, has sold devices in the U.S. to senior living homes, office buildings, manufacturing facilities, and fast food restaurants such as

125. *Id.* at 87.
126. Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?*, ACLU (Oct. 25, 2016), https://www.aclu.org/blog/privacy-technology/internet-privacy/can-consumers-trust-ftc-protect-their-privacy.
127. *Id.*
128. *Id.*
129. *Id.*
130. Jessica Rich, *Give the F.T.C. Some Teeth to Guard Our Privacy*, N.Y. TIMES, (Aug. 12, 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html.
131. *Id.*
132. *Id.*
133. Humerick, *supra* note 118.
134. *Id.*
135. *Id.*
136. *Id.*

Subways and Taco Bell to monitor their employees.[137] PopID checks employees in by asking them to stand in front of a camera that identifies them by their face while measuring their temperature.[138] Through this process, employers are capturing medical information on people along with their facial identification.[139] The problem is that companies usually have discretion in what they do with this data, and these devices could end up being utilized in public places.[140] The U.S. Food and Drug Administration which normally monitors medical and diagnostic devices said it would temporarily permit companies to market unvetted thermal cameras due to the urgency of the pandemic.[141] The American Civil Liberties Union of Hawaii responded to this technology in a letter to government officials by calling the technology "ineffective, unnecessary, rife for abuse, expensive, potentially unconstitutional, and, in a word, terrifying."[142]

Furthermore, Sonde Health developed a voice biometric technique for COVID-19 detection where machine learning is applied to a six-second voice sample to detect respiratory symptoms including coughing, shortness of breath, chest tightness, or pain in order to determine whether an employee can return to work.[143] SHI International, a 5,000-person global technology company, will be implementing this technique.[144] Australia also signed a deal with a drone manufacturer to develop drones with thermal recognition technology that can monitor temperatures, heart rates, respiratory patterns, sneezing, and coughing in coronavirus hotspots.[145]

In the U.S., six states have passed legislation governing biometric information by commercial entities, but most of these laws do not govern the collection of thermal facial recognition data for noncommercial purposes.[146] While some say Section 5 of the FTC Act can provide privacy protections in this area, there is no specific judicial precedent supporting FTC authority to govern the collection or use of thermal information.[147] Furthermore, the FTC has primarily only prosecuted deceptive privacy practices in the past.[148]

137. Emily Waltz, *Entering a Building May Soon Involve a Thermal Scan and Facial Recognition,* IEEE SPECTRUM (June 26, 2020), https://spectrum.ieee.org/the-human-os/biomedical/devices/entering-a-building-may-soon-involve-a-thermal-scan-and-facial-recognition.

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.*

142. *Id.*

143. Chris Burt, *Facial Recognition Temperature Scanning, Wearables and Voice Biometrics Deployed for COVID-19 Spread Prevention*, BIOMETRICUPDATE.COM (Aug. 3, 2020). https://www.biometricupdate.com/202008/facial-recognition-temperature-scanning-wearables-and-voice-biometrics-deployed-for-covid-19-spread-prevention.

144. *Id.*

145. Meredith Van Natta et al., *The Rise and Regulation of Thermal Facial Recognition Technology During the COVID-19 Pandemic*, 7 J. L. & BIOSCIENCES 1, 6 (2020).

146. *Id.* at 8–9.

147. *Id.* at 10.

148. *Id.* at 10–11.

The creation of contact tracing applications is another mitigation technique that highlights the need for federal legislation.[149] Simply put, contact tracing is the process of contacting people who have had contact with someone who tested positive for a disease.[150] The Center for Disease Control (CDC) has stated that "contact tracing" is a key strategy for disease control.[151] The concern is that these applications are not narrowly tailored to achieve the goals of contact tracing and may create unnecessary vulnerabilities to users' privacy.[152] Location data is a big point of concern because location is often difficult to anonymize, has the potential to reveal detailed personal information about users' movements and associations, and is not actually essential for effective contact tracing.[153] Rather than identifying the exact location of users, effective contact tracing can identify whether two users have been in contact through Bluetooth technology signals between the two devices to determine whether the users came in proximity with each other.[154]

However, even with Apple and Google's digital contact tracing technology, which would use Bluetooth technology,[155] the New York Attorney General urged both Apple and Google to take steps to protect consumer information and called upon both tech giants to ensure that existing and third-party contact tracing apps on their respective platforms are not inappropriately collecting user information.[156] Even if tech giants create a minimally invasive contact tracing app, Americans will hesitate to allow their smartphones to become contact tracing devices because of the worry that the app may also be tracking their other behaviors.[157] Researchers estimated that more than sixty percent of people with smartphones must use the contact tracing app for it to be effective.[158]

Despite the potential of contact tracing apps to mitigate COVID-19, Americans remain distrusting due to uneven privacy regulations that cause

149. Shari Lewis, *Contact Tracing Raises Privacy Issues for Businesses to Consider*, LAW.COM (Oct. 19, 2020), https://www.law.com/newyorklawjournal/2020/10/19/contact-tracing-raises-privacy-issues-for-businesses-to-consider/.

150. *Id.*

151. Cynthia Cole, Brooke Chatterton, Natalie Sanders & Baker Botts, *The Safety of Privacy: Increased Privacy Concerns May Prevent Effective Adoption of Contact Tracing Apps*, LAW.COM (Aug. 18, 2020), https://www.law.com/legaltechnews/2020/08/18/the-safety-of-privacy-increased-privacy-concerns-may-prevent-effective-adoption-of-contact-tracing-apps/.

152. Chanley Howell & Chloe Talbert, *Privacy Risks and Implications of Contact Tracing Apps and Related Technologies*, NAT'L L. REV. (Aug. 25, 2020), https://www.natlawreview.com/article/privacy-risks-and-implications-contact-tracing-apps-and-related-technologies.

153. *Id.*

154. *Id.*

155. *Id.*

156. Press Release, Letitia James, New York Attorney General, Attorney General James Urges Apple and Google to Take Steps to Protect Consumers Using Coronavirus Contact Tracing Apps (June 15, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-urges-apple-and-google-take-steps-protect-consumers-using.

157. Howell, *supra* note 147.

158. *Id.*

individuals to doubt that their information will not be used against them.[159] Even in the midst of a pandemic, the public remains skeptical of the U.S. government's use of data, with a majority of Americans saying that data collection in the U.S. will "not make much of a difference" in stopping the spread of COVID-19.[160] Paul Schwartz, a privacy scholar, concluded that "public use of these apps ultimately depends on the extent of trust in them."[161] The nation's efforts to mitigate this pandemic will ultimately be hindered by the U.S. public's distrust.[162]

Data collection as a result of COVID-19 is happening whether Americans like it or not. Government agencies have put into place – or contemplated – a variety of tracking and surveillance technology that range from geolocation tracking to facial recognition programs that analyze pictures to determine whether people came in contact with a COVID-19 positive person.[163] Furthermore, while Zoom Video (Zoom) provided an essential service during the unprecedented health crisis, privacy concerns surfaced.[164] Zoom reserves the right to change its privacy policy at any time and Consumer Reports speculated that Zoom could use users' personal data for targeted advertising campaigns and even develop facial recognition algorithms.[165] Moreover, Zoom allows administrators to access real-time dashboards of user activity, which allows them to see users' doings and activities.[166] Zoom has also been known to give third parties, such as Facebook, personal data for what it considers "business purposes."[167] The complexity and lengthiness of Zoom's terms of agreements and the lack of other options, especially if a user's workplace only uses Zoom, cause users to have no other option but to use Zoom.[168]

The fragmented state of data privacy law and vague guidance on regulation in the U.S. makes for an unsuccessful shield against Zoom's privacy practices.[169] It has been observed that the FTC "often investigates cases where there has been a clear lack of informing consumers of a privacy

159. *Id.*

160. Müge Fazlioglu, *Déjà Vu? The Politics of Privacy Legislation During COVID-19*, IAPP (May 21, 2020), https://iapp.org/news/a/deja-vu-the-politics-of-privacy-legislation-during-covid-19/.

161. *Id.*

162. *Id.*

163. John Neocleous, *Expert Analysis: Data Collection, Personal Privacy, and COVID-19 Contact Tracing How the Virus and New Tech Triggered Thorough Review and Clarification Surrounding Privacy Laws*, A.B.A. (June 4, 2020), https://www.americanbar.org/groups/business_law/publications/blt/2020/06/expert-analysis/.

164. Michael Goodyear, *The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and The Fragmented State of U.S. Data Privacy Law*, 10 HOUS. L. REV. 76, 81–82 (2020).

165. *Id.* at 80.

166. *Id.* at 78.

167. *Id.* at 79.

168. *Id.* at 77–78.

169. *Id.*

practice in advance."[170] Since Zoom lays out its privacy practices in its privacy policy, it is questionable whether the FTC would be able to investigate Zoom's practices.[171] However, it is not surprising that users rarely read privacy policies; it would take about seventy-six work days for a user to read every privacy policy he or she encountered during a year.[172]

Contact tracing apps raise confusions around privacy such as data ownership, rules for third-party apps, and how to enforce a system for deleting the data.[173] In the absence of a federal privacy law, the U.S. resorts to HIPAA, a sector-specific approach, for guidance.[174] However, not all health data is covered under HIPAA and companies that heavily invest in contact tracing such as Google, Apple, and Microsoft are not held to HIPAA standards.[175] State-specific laws such as the CCPA and New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) are only specific to those states.[176] Even in California, only 26% of respondents said they were making an effort to meet CCPA requirements.[177] Other states with high COVID-19 cases, such as South Carolina with over 95,000 confirmed cases as of August 2020, are prevented from deploying contact-tracing apps.[178] The lack of uniformity between states makes contact tracing difficult, especially when residents are allowed to travel between states.[179]

The different types of laws in place clash and make it difficult to implement contact tracing apps without federal legislation. For instance, while the Illinois Biometric Information Act requires caution when collecting biometric data such as temperature measurement with facial recognition,[180] the CCPA could require disclosure of biometric data.[181] Federal legislation would ensure the privacy of consumers' personal health and ensure

170. *Id.* at 82.
171. *Id.*
172. *Id.* at 78.
173. *Rush to Contact Tracing Apps Expose Conflict*s, IEEE INNOVATION AT WORK, https://innovationatwork.ieee.org/rush-to-contact-tracing-apps-expose-conflict-between-data-privacy-and-public-health (last visited Dec. 25, 2020) [hereinafter IEEE, *Rush to Contact Tracing*].
174. *Id.*
175. Alfred Ng, *A National Privacy Law Would Have Helped the U.S. Deal with COVID-19, Lawmakers Say*, CNET (Sept. 23, 2020), https://www.cnet.com/health/a-national-privacy-bill-really-would-have-helped-the-us-deal-with-covid-19.
176. IEEE, *Rush to Contact Tracing*, *supra* note 173.
177. *Id.*
178. *Id.*
179. *See id.*
180. Eliana Theodorou, *COVID-19 and the Illinois Biometric Information Privacy Act*, OUTTEN & GOLDEN (May 13, 2020), https://www.outtengolden.com/blog/2020/05/covid-19-and-illinois-biometric-information-privacy-act.
181. Anthony Zaller, *Employee Biometric Data Issues Under California Law*, CAL. EMP. L. REP. (Feb. 7, 2020), https://www.californiaemploymentlawreport.com/2020/02/employee-biometric-data-issues-under-california-law.

confidence and trust in technology.[182] Julie Brill, Microsoft's chief privacy officer and former FTC commissioner, emphasized that the lack of a federal privacy law creates difficulties in dealing with pandemics and in providing people with the trust that they need to allow companies, governments, and other organizations to respectfully and responsibly use data to address these crises.[183] The COVID-19 pandemic further amplified the need of comprehensive federal privacy laws.[184] Further, in September 2020, Congress held a committee hearing titled "Revisiting the Need for Privacy Legislation," which again shows that there is a dire need for comprehensive federal legislation in data privacy.[185]

IV. CURRENTLY PROPOSED DATA PRIVACY LAWS: GENERAL LEGISLATION AND PANDEMIC-RESPONSIVE LEGISLATION

With the burden on businesses imposed by the increase of privacy and data protection laws such as data breach notification obligations and requirements for data transferring imposed by international data protection laws such as the EU General Data Protection Regulation (GDPR), the U.S. is overdue for a comprehensive, non-scattered federal privacy bill.[186] While there has been a good amount of proposed laws, none have been officially passed and are not likely to gain traction.[187] Furthermore, while there have been three proposed data privacy acts protecting data collected through contact tracing and exposure notification,[188] these laws are insufficient and require re-examination.

A. GENERAL PROPOSALS GOVERNING DATA PRIVACY

Three privacy legislation proposals are the Consumer Online Privacy Rights Act (COPRA), the Consumer Data Privacy Act (CDPA), and the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE Data Act).[189] Commenters have noted that "[i]n the end...[t]he pandemic consumed much of the legislative energy and made it difficult to overcome partisan polarization.[190]

182. *Stronger Data Privacy Laws Called Essential to Effective Contact Tracing*, CRIME REP. (Sept. 25, 2020), https://thecrimereport.org/2020/09/25/stronger-data-privacy-laws-called-essential-to-covid-19-contact-tracing/.

183. NG, *supra* note 175.

184. *Id.*

185. KERRY & CHIN, *supra* note 6.

186. Wendy Zhang, *Comprehensive Federal Privacy Law Still Pending*, NAT'L L. REV. (Jan. 22, 2020), https://www.natlawreview.com/article/comprehensive-federal-privacy-law-still-pending.

187. *Id.*

188. JOHNATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10501, "TRACING PAPERS": A COMPARISON OF COVID-19 DATA PRIVACY BILLS, at 1 (2020).

189. Kerry, *supra* note 6.

190. *Id.*

COPRA, introduced by the Democratic party, sets a floor for liability and creates a "private right of action that presumes that privacy violations are concrete injuries, permitting consumers to directly seek civil damages."[191] COPRA has fairly broad applicability, but it excludes entities that can establish all of the following for the preceding three calendar years: "(1) average gross revenues of less than $25 million per year; (2) annual processing of covered data of fewer than 100,000 individuals, households or devices; and (3) less than 50% of revenue derived from transferring covered data."[192] The bill also exempts entities subject to other federal privacy laws such as HIPAA.[193] Key provisions of COPRA include requiring individual consent for certain data processing activities, the right to opt-out of certain transfers of covered data to a third party, the right to correct and delete covered data, and the right to have entities provide individuals with their own covered data upon request and name any third party to which it has been transferred in exchange for consideration or for a commercial purpose.[194]

COPRA also requires covered entities to publish a privacy policy that describes the company's data processing and transferring activities.[195] It also requires entities to "undertake vulnerability assessments, employee training, and retention and disposal procedures."[196] COPRA also enforces obligations for CEOs and other executives that are large data holders – such as companies that "process or transfer sensitive covered data of more than 5 million individuals, devices or households, or that process or transfer sensitive covered data for more than 100,000 individuals, devices or households."[197] On top of this, COPRA introduces a "duty of loyalty" responsibility to stop entities from engaging in deceptive or harmful practices.[198] COPRA would supersede any state law in direct conflict, but would allow any law that afforded a greater level of protection.[199]

The SAFE Data Act was introduced by Republican Senators.[200] In contrast to Democratic privacy bills such as COPRA, the SAFE Data Act does not contain a private right of action and would preempt state privacy

191. Susan Steinman, *A Plethora of Privacy Bills*, TRIAL MAG., Mar. 2020, at 54.

192. Kaylee Bankston & Jesse Brody, *Framing a Federal Privacy Standard: Congressional Efforts Continue,* JD SUPRA (Dec. 13, 2019), https://www.jdsupra.com/legalnews/framing-a-federal-privacy-standard-81107.

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

197. *Id.*

198. *Id.*

199. David Saunders & Allison Glover, *INSIGHT: A Federal Privacy Bill May Be Closer Than Once Thought*, BLOOMBERG L. (Feb. 14, 2020), https://news.bloomberglaw.com/privacy-and-data-security/insight-a-federal-privacy-bill-may-be-closer-than-once-thought.

200. Megan Brown et al., *Federal Privacy Law Efforts Move Forward in Congress*, JD SUPRA (Oct. 5, 2020), https://www.jdsupra.com/legalnews/federal-privacy-law-efforts-move-19243.

laws.[201] The bill would create rights to transparency, access, deletion, correction, and portability, while requiring opt-in consent to process or transfer "sensitive covered data," including biometric information and geolocation data.[202] This type of development is significant in order to encompass innovation in technology such as algorithms powered by artificial intelligence (AI).[203] The Act also prohibits "opaque" algorithms[204] unless entities (i) notify users of the algorithm, and (ii) avail an "input-transparent algorithm" that users can easily switch to.[205]

B. PROPOSED PRIVACY LAWS AS A RESULT OF COVID-19

The COVID-19 Consumer Data Protection Act (CCDPA), the Public Health Emergency Privacy Act (PHEPA), and the Exposure Notification Privacy Act (ENPA) were proposed in response to data collection during the pandemic.[206] Each bill requires a covered entity to (1) not disclose or transfer an individual's data for any purposes other than those enumerated in the bills, (2) publish a privacy policy to provide notice as to the type of data the entity collects, the purpose of the collection, how the entity will use collected data, and an individual's rights with respect to the data, (3) obtain an individual's affirmative express consent before collecting the individual's data, (4) provide an individual with the right to opt-out of collection by withdrawing consent, (5) delete an individual's data on request after a set period and (6) safeguard an individual's data by adopting appropriate data security measures.[207] The proposed bills leave significant gaps.

1. CCDPA

The CCDPA, introduced by U.S. Republican Senators, covers organizations, including businesses under the FTC's jurisdiction as well as non-profits and common carriers.[208] It covers data including geolocation data, proximity data, persistent identifiers that can be used to identify a user over time, such as IP addresses or device IDs, and personal health information.[209] Its goals are to track the spread, symptoms, or signs of COVID-19, measure

201. *Id.*
202. *Id.*
203. *Id.*
204. An opaque algorithm is one that determines the order or manner information is shown to users on an internet platform based on those users' information that was not expressly provided. Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, SAGE J. (Jan. 6, 2016), https://journals.sagepub.com/doi/10.1177/2053951715622512.
205. BROWN, *supra* note 200.
206. GAFFNEY, *supra* note 188, at 1.
207. *Id.* at 2–3.
208. 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), https://www.jdsupra.com/legalnews/federal-privacy-law-in-response-to-26186.
209. *Id.*

compliance with social distancing guidelines, and conduct contact tracing.[210] The enforcers would be the FTC or state attorney generals.[211] The CCDPA covers entities or persons engaged in a covered activity that is (1) subject to regulation by the FTC, (2) a common carrier as defined in the Communications Act of 1934, or (3) a nonprofit organization.[212]

The CCDPA has room to grow. For one, it would preempt state laws "related to" the processing of covered data such as location, proximity, persistent identifiers, and health information, for a covered purpose such as tracking COVID-19, measuring social distancing, and contact tracing.[213] As a result, certain state citizens' legal rights would be cut back.[214] For example, Californians' existing legal rights to access, delete, or opt-out of the sale of data collected for COVID-19 purposes would be cut back and Illinoisans' right to be free from unconsented biometric surveillance for COVID-19 purposes would also be preempted.[215] Further, the CCDPA would cut back existing state laws that address medical privacy, information security, data breach notification, and unfair trade practices.[216] The "laboratories of democracy"[217] would be violated since it would stifle novel social and economic experiments in mitigating COVID-19.[218] Secondly, the CCDPA does not provide for a private right of action.[219]

Lastly, the CCDPA does not cover data collected concerning anyone "permitted to enter a physical site of operation" of the entity, including employees, vendors, and visitors.[220] It also does not cover data collected by employers to determine whether employees may enter a physical location.[221] This will in turn allow businesses to fire employees so long as the businesses claim that they are trying to prevent a workplace outbreak.[222] Further, the CCDPA does not apply to service providers that do not themselves collect covered data, but transfer or process data for covered entities.[223]

210. *Id.*
211. *Id.*
212. GAFFNEY, *supra* note 188, at 2.
213. Adam Schwartz, *Two Federal COVID-19 Privacy Bills: A Good Start and a Misstep*, ELECTRONIC FRONTIER FOUND. (May 28, 2020), https://www.eff.org/deeplinks/2020/05/two-federal-COVID-19-privacy-bills-good-start-and-misstep.
214. *Id.*
215. *Id.*
216. *Id.*
217. A term popularized by U.S. Supreme Court Justice Louis Brandeis in *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) to describe how a state may, if its citizens choose, to serve as a laboratory and try novel social and economic experiments without risk to the rest of the country. The concept behind the term is that there exists a system of state autonomy where state and local governments can create and test laws and policies at the state level.
218. Schwartz, *supra* note 213.
219. *Id.*
220. GAFFNEY, *supra* note 188, at 2.
221. NGUYEN, *supra* note 208.
222. SCHWARTZ, *supra* note 213.
223. NGUYEN, *supra* note 208.

2. PHEPA

PHEPA, introduced by Democratic U.S. Senators, governs public and private entities that collect Emergency Health Data (EHD).[224] EHD includes personal health information, geolocation data, proximity data demographic data, and contact information.[225] PHEPA, unlike the CCDPA, is not limited to private entities and would regulate some governmental use, collection, and disclosure of EHD.[226] However, PHEPA does not cover health care providers, public health authorities, service providers, and persons acting in their individual or household capacity.[227] PHEPA requires opt-in consent and data minimization, and limits data disclosures to the government.[228] Unlike the CCDPA, PHEPA has a strong private right of action and does not preempt state laws.[229] However, PHEPA still leaves an opportunity for discrimination for those who decide to not opt-in in the areas of access to employment, public accommodations, and government benefits.[230] It also contains overly broad exemptions for manual contact tracing programs that will gather a vast amount of personal data that will be held by private corporations.[231] Furthermore, although PHEPA exempts public health authorities, government officials should be held to the bill's rules as well.[232]

3. The ENPA

Unlike CCDPA and PHEPA, ENPA is not limited to the current public health emergency and will be in effect after the COVID-19 pandemic.[233] However, ENPA applies only to automated exposure notification service-collected data, meaning data that is collected through a tool for "digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease."[234] ENPA explicitly states that it would not preempt any state laws.[235] Since ENPA only applies to exposure notification systems, such as contact tracing apps, other digital pandemic response tools are not covered under the bill.[236] The U.S. is already developing a range of digital response tools outside of exposure notification systems.[237] These tools

224. *Id.*
225. *Id.*
226. *Id.*
227. GAFFNEY, *supra* note 188, at 2.
228. Schwartz, *supra* note 213.
229. *Id.*
230. *Id.*
231. *Id.*
232. *Id.*
233. GAFFNEY, *supra* note 188 at 2.
234. *Id.*
235. *Id.*
236. Christine Bannan, *Congress Considers Three Bills Addressing Privacy Protections During COVID-19 Crisis*, NEW AM. (July 14, 2020), https://www.newamerica.org/oti/blog/congress-considers-three-bills-addressing-privacy-protections-during-covid-19-crisis.
237. *Id.*

include QR codes and "immunity passports" to track users' movements.[238] ENPA leaves out important proponents that are necessary to mitigate future public health emergencies.[239]

4. States: COVID-19 Responsive Legislation

States have made efforts to advance COVID-19 data privacy legislation as well.[240] For instance, the New York State Senate Chairman of Consumer Protection advanced a new bill to protect the privacy rights of New Yorkers amid the pandemic.[241] This bill was a response to companies looking to technology in order to monitor potential risks for COVID-19 exposure.[242] The bill imposes strict limits on data usage; any technology that involves collection, sharing, and use of health information.[243] Furthermore, a new biometrics privacy ordinance has taken effect across New York City.[244] The ordinance protects customer biometric data by providing safeguards from businesses that collect such information. Businesses in New York City are now required to conspicuously post notices and signs at their doors to warn customers of how their data will be collected.[245] Businesses are also barred from selling, sharing, or otherwise profiting from biometric information collected. This ordinance is not perfect, as it does not apply to government agencies, but it shows the increasing acknowledgment of privacy issues that will come out of the pandemic.

C. PRIVACY RESPONSES TO REOPENING

With offices reopening, there is a thin line between ensuring employee safety and protecting their privacy.[246] With a plethora of laws, there is a further complication in creating balance.[247] Hawaii, Montana, and Oregon passed laws favoring worker privacy during the pandemic; the three states have set restrictions for employers in tracking the location and personal

238. *Id.*
239. *Id.*
240. Kevin Thomas, *COVID-19 Data Privacy Legislation Passes New York State Senate*, CONSUMER PROT. COMM. (July 23, 2020), https://www.nysenate.gov/newsroom/press-releases/kevin-thomas/covid-19-data-privacy-legislation-passes-new-york-state-senate.
241. *Id.*
242. *Id.*
243. *Id.*
244. *See generally* N.Y.C. Admin. Code §§ 22-1201–22-1205 (2021).
245. Bram Schumer & Boris Segalis, *NYC Enacts Biometric Data Disclosure Rules and Restrictions*, JD SUPRA (May 19, 2021), https://www.jdsupra.com/legalnews/nyc-enacts-biometric-data-disclosure-9315634.
246. Paige Smith & Chris Marr, *As Offices Reopen, State Laws Thread Worker Privacy and Safety*, BLOOMBERG L. (July 21, 2021), https://news.bloomberglaw.com/health-law-and-business/as-offices-reopen-state-laws-thread-worker-privacy-and-safety.
247. *Id.*

information of workers, and Montana is preventing employers from mandating the COVID-19 vaccination.[248]

As the first U.S. city to require proof of vaccination to enter businesses, New York City implemented a system requiring people to show that they received at least one coronavirus vaccine shot. While this gatekeeping will act as an added layer of precaution, new digital privacy concerns will be raised.[249] New York's tactic includes the options of paper vaccination cards, the NYC Covid Safe app, or the Excelsior Pass app, developed by IBM.[250] Currently, there are no laws safeguarding data uploading onto an app.[251] The Excelsior Pass app also proposes to add a "Phase 2" which may include adding more personal information and further health records that businesses can obtain upon entry.[252] IBM indicated that it uses "blockchain technology and encryption to protect user data," but failed to expand on how that works.[253]

One example of how the collection of personal data through apps can go awry was when Singapore officials initially stated that data would be used solely for contact tracing, but ultimately used the data to aid in criminal investigations.[254] Although there may not have been noted occurrences of the same incidents in the U.S., businesses using the Excelsior Pass Plus, which discloses whether an individual is vaccinated and also information about when and where they received their shot, it may be able to save or store the information contained.[255]

V. THE INAPPLICABILITY OF PROPOSED LAWS TO FUTURE TECHNOLOGY AND EVENTS

It is important to analyze how existing and proposed laws would play out in future data privacy issues such as with 5G, the new generation of wireless networking technology that promises 600 times faster speeds than 4G.[256] Cloud computing security is essential because it goes hand in hand with 5G's success since many industries that will use 5G rely on cloud computing to share large files and large numbers of files between devices.[257] It is unclear

248. *Id.*
249. Erin Woo & Kellen Browning, *New York City's Vaccine Passport Plan Renews Online Privacy Debate*, N.Y. TIMES (Aug. 4, 2021), https://www.nytimes.com/2021/08/04/technology/vaccine-passport-ny-privacy.html.
250. *Id.*
251. *See id.*
252. *Id.*
253. *Id.*
254. *Id.*
255. *Id.*
256. Klint Finley & Joanna Pearlstein, *The WIRED Guide to 5G*, WIRED (Sept. 10, 2020), https://www.wired.com/story/wired-guide-5g/.
257. Alex Marginean, *How The 5G Network Will Impact Cloud Computing*, PICANTE (Apr. 10, 2020), https://picante.today/technology/2020/04/10/141905/how-the-5g-network-will-impact-cloud-computing/.

whether the FTC would govern privacy in the cloud computing area since the FTC usually regulates e-commerce issues.[258] Regardless, relying on government agencies to address the failure of companies to protect consumer data in the cloud may be ineffective since individual consumers would not be clearly represented – government agencies address problems on an ad hoc basis when a data breach occurs.[259] Regulation in this area, prior to any data breach at all, would be more beneficial to consumers.[260]

Proposed bills to address COVID-19 do not suffice to address the current and future public health emergencies. There are two main divergences among the CCDPA, PHEPA, and ENPA – whether there should be a private right of action and whether to preempt state law.[261] Moreover, the proposed laws may not have much impact on state-run digital contact-tracing apps, which are necessary to mitigate future emergencies.[262] The CCDPA would only apply to private entities and both PHEPA and ENPA exclude public health authorities from their covered entities.[263] Congress should consider adding public health authorities to the list of covered entities. Moreover, the CCDPA and PHEPA will not apply once the COVID-19 pandemic is over.[264]

While ENPA is strong, it is limited in scope.[265] While the bill protects health data by permitting the use and disclosure of collected data only when it is necessary to implement an exposure notification service for public health purposes, it lacks a private right of action.[266] A private right of action would enable individuals to enforce their rights.[267] Furthermore, while the bill prevents discrimination against individuals for public services and accommodations, it does not extend similar protections to employment or voting.[268] Working in the short-term can bear implications and repercussions.[269] Even with unforeseen events such as the COVID-19 pandemic, there needs to be a careful crafting of legislation to ensure that laws encompass a range of tools in order to sufficiently address future emergencies.

258. Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 435 (2013).
259. *Id.* at 436.
260. *Id.*
261. Rebecca Kern & Daniel R. Stoller, *Bipartisan Privacy Talks Split With Second Senate GOP Bill (1)*, BLOOMBERG GOV'T (Mar. 12, 2020), https://about.bgov.com/news/bipartisan-privacy-talks-split-with-second-senate-gop-bill-1/.
262. JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., R46542, DIGITAL CONTACT TRACING & DATA PROTECTION LAW, at 37 (Sept. 24, 2020).
263. *See* CCDPA § 2(7); PHEPA § 2(4); ENPA § 2(11).
264. GAFFNEY, *supra* note 188, at 2.
265. Bannan, *supra* note 236.
266. *Id.*
267. *Id.*
268. *Id.*
269. *Id.*

VI. PROPOSED SOLUTION

Four big hurdles in adopting new privacy laws are: (1) whether state laws should be preempted, (2) whether there should be a private right of action, (3) the need for provisions that directly address privacy over health data gathered through health emergency mitigation technologies, and (4) the need to minimize disparate impact. There needs to be comprehensive federal privacy law that preempts scattered state laws, provides a way of redress for victims, protects data collected by new technologies, and minimizes disparate impact.

A. PREEMPTION OF STATE LAWS

Consistent national privacy standards benefit both individuals and industries. A person's privacy should not depend on the state they are in. Today's digital world is borderless; governing digital data based on state borders will not suffice. A set of privacy laws that preempt inconsistent state laws would allow for easier compliance from industries and provide individuals with consistent data protection. There is an argument that state privacy laws allow states to be the "laboratories of democracy" and should be able to try novel experiments without risk to the rest of the country.[270] However, this problem is swallowed by the issues raised through a scattershot of state privacy laws. Any state involvement should be supplementary to federal law and should be evaluated after a sunset provision period. Enacting a sunset provision for preemption would allow Congress to revisit the legislation and determine whether there is a need for state laws. If there is a need for state law, the federal law should not be extinguished, but its provisions should be adjusted in order to maintain a uniform "floor" of privacy protection. In other words, state laws should only be permitted to strengthen the federal law after it is adjusted. There is no doubt that the U.S. is in need of federal privacy legislation;[271] the sunset provision allows for the implementation of federal legislation while taking state police powers into consideration.

B. PROVIDING REDRESS THROUGH A REVISED PRIVATE RIGHT OF ACTION

A private right of action has been polarized and treated as an all-or-nothing proposition in proposals.[272] Any federal privacy legislation will be

270. Jeff Sovern, *Why a U.S. Federal Privacy Law Could Be Worse Than No Law at All*, FAST COMPANY (May 18, 2019), https://www.fastcompany.com/90352025/why-a-u-s-federal-privacy-law-could-be-worse-than-no-law-at-all.

271. Zhang, *supra* note 181.

272. Cameron Kerry, *Private Lawsuits Are a Necessary Expedient in Privacy Legislation*, THE HILL (June 11, 2020), https://thehill.com/opinion/technology/502209-private-lawsuits-are-a-necessary-expedient-in-privacy-legislation.

hindered if both Democrats and Republicans have power to stop the other; it will take compromise on a private right of action in order to pass legislation.[273] The solution is to allow for individual enforcement for some provisions of the privacy law, but not for the entirety of it. For example, Congress can allow for private enforcement of the right to delete or correct data, but not for provisions, such as data portability requirements, that litigation would not resolve. Data portability litigation is often unfair and counterproductive because it ranks as one of the most difficult privacy compliance obligations.[274]

Another safeguard to a solution under the private right of actions is to require an effective regulator to investigate and process complaints prior to permitting someone to sue. The FTC is not the appropriate regulator. In most of the enforcement actions regarding internet privacy, the FTC did not levy civil penalties because it lacked such authority for those violations.[275] Instead of the FTC, the creation of a separate group would be beneficial. This group would focus on promoting data protection and privacy innovations across sectors and prepare the American government for technological advancements by advising Congress on emerging privacy and technology developments. Although Congress is one of the most powerful representative assemblies, its lack of knowledge on technology and modern digital infrastructure was revealed during Congress's hearings on Facebook.[276] The group would also be the face of the U.S. at international forums on data privacy. The establishment of such a group will allow for privacy law enforcement and keep the nation's government officials abreast on privacy issues.

This new group will operate under similar agency models in the U.S. such as the Equal Employment Opportunity Commission (EEOC). The EEOC requires an investigation of a claim before filing a lawsuit. The commission will either mediate the dispute, file a lawsuit on the employee's behalf, or close the case and issue a "Right to Sue Letter."[277]

273. *Id.*

274. *IAPP-EY Annual Privacy Governance Report 2017*, IAPP, https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf (last visited Sept. 23, 2021).

275. GOV'T ACCOUNTABILITY OFF., INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY (2019), https://www.gao.gov/assets/gao-19-52.pdf.

276. Lorelei Kelly & Robert Bjarnason, *Our 'Modern' Congress Doesn't Understand 21st Century Technology*, TECHCRUNCH.COM (May 6, 2018), https://techcrunch.com/2018/05/06/our-modern-congress-doesnt-understand-21st-century-technology/.

277. *See Filing a Lawsuit*, EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/filing-lawsuit (last visited Dec. 24, 2020).

C. PROTECTION OVER DATA COLLECTED THROUGH TECHNOLOGY USED FOR EMERGENCY MITIGATION EFFORTS

ENPA is relevant because it will be in effect and govern future health data collection even after the COVID-19 pandemic ends. However, ENPA only applies to automated exposure notification service-collected data and excludes other prevalent mitigation tools that are being deployed such as thermal imaging and QR codes used to track movements.[278] As the only pandemic-induced law that will be enforced after the COVID-19 pandemic, ENPA needs to expand its scope to other data-collecting technologies such as immunity passports and QR codes. Immunity passports, an idea that the U.S. is heavily considering, are given to those who have recovered and tested positive for antibodies, allowing them the privilege to return to work, and travel.[279] QR Codes, another mitigation effort that the U.S. is considering, are codes on a user's smartphone to control their entrance into public places based on their COVID-19 health status.[280] China has announced that the QR-code tracking system is likely to remain in place after the pandemic ends.[281] As technology continues to evolve, there will surely be new data-collection methods that ENPA needs to govern. The U.S. cannot simply work in the short term.

In addition, ENPA needs to be strengthened with further provisions. One important addition is user-friendly privacy policies. As mentioned, lengthy agreements are often roadblocks for users and drive distrust in the U.S.[282] ENPA needs to require user-friend privacy policies that clearly describe the data being collected, how it is being used, and how it is being protected. Developers of mitigation-driven technologies should be required to implement safeguards such as limiting the spread of data to sharing with state public health authorities such as the CDC.

ENPA also needs to address the retention of data. Considering the fact that data has been misused for many purposes, such as immigration issues,[283] there should be an exit plan that ensures that data will not be used beyond mitigation purposes. The solution is to require data collection to end when hospitalization rates drop below a certain percentage or when a certain percentage of the population is vaccinated or immune.

278. Bannan, *supra* note 231.

279. Natalie Kofler & Françoise Baylis, *Ten Reasons Why Immunity Passports are a Bad Idea*, NATURE (May 21, 2020), https://www.nature.com/articles/d41586-020-01451-0.

280. *Id.*

281. *Id.*

282. Kelly, *supra* note 21.

283. Erica Posey & Rachel Levinson-Waldman, *What Lurks Behind All That Immigration Data*, ACLU (Apr. 4, 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/what-lurks-behind-all-immigration-data.

D. MINIMIZATION OF DISPARATE IMPACT

As digital tools are being deployed to help reopen the nation amid COVID-19, legislators should work to prevent future harm to communities that are already suffering disproportionately from the virus and economic hardships.[284] The proposed COVID-19 related bills do not restrict the way law enforcement or other government entities can access or use data collected for contact tracing purposes, which in turn enables that data to be inappropriately used.[285] Moreover, the CCDPA does not contain any prohibition on discriminatory uses of data collected for contact tracing purposes.[286] This allows for data to be used in adverse decision-making about an individuals' access to employment, housing, public accommodations, and voting.[287]

Comprehensive federal privacy legislation would set forth principles that prevent disparate impact. Legislation should include a provision that prohibits data from being used to discriminate against a person for employment, housing, public accommodations, or voting purposes. A private right of action would be invoked if organizations violate the provision. A board within the new group comprised of professionals in the area of discriminatory impact on underserved communities should also be established to oversee this provision.

CONCLUSION

It is clear that the U.S. needs federal privacy legislation. This pandemic exacerbated the complications that can arise without one. While the COVID-19 pandemic has brought the issues further to the legislative table, the existing and proposed laws will not suffice in a world comprised of data-collecting technologies. There will also be future emergencies that require health data collection. The U.S. must lay a strong, functional, federal data privacy law to protect its citizens.

Marissa Wong[*]

284. Bannan, *supra* note 231.
285. *Id.*
286. *Id.*
287. *Id.*

* B.B.A. Baruch College Zicklin School of Business, May 2015; J.D., Brooklyn Law School, 2021. I would like to thank the entire staff of the Brooklyn Journal of Corporate, Financial & Commercial Law for their hard work and feedback. Thank you to my family and friends for their encouragement and support.