Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 18
Issue 1 *The Law of Torts: Duty, Design, & Conflicts A Festschrift in Honor of Aaron Twerski*

Article 12

12-30-2023

It's Finally Time for A National Data Privacy Law: A Discussion of the American Data Privacy And Protection Act (ADPPA)

Erin J. An

IT'S FINALLY TIME FOR A NATIONAL DATA PRIVACY LAW: A DISCUSSION OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT

ABSTRACT

Millions of Americans face unprecedented privacy risks related to their data, often without their awareness. With the increasing value of consumer data and its growing utilization by businesses, there is a growing demand for greater transparency and privacy protections. As of 2023, no comprehensive federal law governs data privacy in the United States, leaving citizens with limited protections. Introduced to Congress on June 21, 2022, the American Data and Privacy Protection Act (ADPPA) successfully passed the House of Representatives Committee on Energy and Commerce, making it the furthest a national comprehensive data privacy bill has progressed through the federal legislative process compared to any other proposed bill. This Note discusses the ADPPA, specifically its notable features and the changes it has seen in Congress. This Note then provides a comparative analysis of other modern data privacy laws, such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR). Furthermore, this Note reviews the implications of the ADPPA on businesses and consumers if it is signed into law. Finally, this Note concludes by proposing solutions lawmakers could consider to mitigate criticisms the bill has received.

INTRODUCTION

On August 29, 2022, the Federal Trade Commission (FTC) filed a lawsuit against data broker Kochava, Inc., for allegedly acquiring and selling consumers' geolocation data from millions of mobile devices.[1] This data, which could be used to track individuals' movements to and from "sensitive" locations—such as abortion clinics, homeless shelters, addiction recovery facilities, and places of worship—was sold to various entities.[2] The FTC claimed that Kochava's sale of this data exposed individuals to various threats, including stalking, stigma, physical violence, discrimination, and job loss.[3] The FTC sought to enjoin Kochava's sale of this data and to force the data broker to delete the collected data.[4] Similarly, on January 13, 2021, the FTC sued Flo Health, Inc., a menstrual period and fertility tracking app with

1. Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

2. *Id.*

3. *Id.*

4. *Id.*

over 100 million users, for allegedly disclosing the personal health information of its users to outside data analytics providers, despite claiming that such information would be kept private.[5] During the same year, data from the location-based gay dating app Grindr was leaked, linking a Catholic priest to the app.[6] Also in that year, a cyberattack on T-Mobile exposed the sensitive information of more than forty million people, including customers' names, social security numbers, and PIN numbers.[7] These cases are just a few examples of the numerous issues involving exposed personal data across various industries.

More than ever before, millions of Americans are at risk of privacy concerns involving their data—most of the time without them even knowing it. As consumer data is becoming exponentially more valuable, the demand for privacy and transparency regarding data collection, confidentiality, and transmission is also growing. Currently, there is no comprehensive federal law governing data privacy in the United States, leaving citizens with limited protections.[8] However, things may change soon. The American Data and Privacy Protection Act (ADPPA) was introduced to Congress on June 21, 2022, and passed the House of Representatives Committee on Energy and Commerce by a vote of 53-2, making it the furthest a national comprehensive data privacy bill has progressed through the federal legislative process compared to any other proposed bill.[9] Interestingly, this bill received rare bipartisan votes, and while there is still a long way to go, passage of this bill could have profound effects on the privacy landscape in the United States.[10]

Part I of this Note provides background on the current state of data privacy laws in the United States, including sectoral federal and state privacy laws, as well as on the European Union's (EU) General Data Protection Regulation (GDPR), the global standard for national privacy laws. Part II is an overview of the ADPPA and includes a discussion of the bill's notable

5. Press Release, Fed. Trade Comm'n, Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about [hereinafter Fertility-Tracking App Press Release]

6. Sara Morrison, *This Outed Priest's Story Is a Warning for Everyone About the Need for Data Privacy Laws*, VOX (July 21, 2021, 7:20 P.M.), https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting.

7. Isabella Grullón Paz, *T-Mobile Says Hack Exposed Personal Data of 40 Million People*, N.Y. TIMES (Aug. 18, 2021), https://www.nytimes.com/2021/08/18/business/tmobile-data-breach.html.

8. Anne Toomey McKenna, *A New US Data Privacy Bill Aims to Give You More Control Over Information Collected About You—and Make Businesses Change How They Handle Data*, THE CONVERSATION (Aug. 23, 2022, 2:27 PM), https://theconversation.com/a-new-us-data-privacy-bill-aims-to-give-you-more-control-over-information-collected-about-you-and-make-businesses-change-how-they-handle-data-188279.

9. Matt Davis, *What Is the ADPPA (American Data Privacy and Protection Act)?*, OSANO (Aug. 5, 2022), https://www.osano.com/articles/adppa.

10. *Id.*

features and amendments made during its progression through Congress. Part III discusses the implications for businesses and consumers if the ADPPA is signed into law, such as the steps required to comply with the law and the rights it affords consumers. Finally, Part IV addresses criticisms the bill has received thus far, followed by suggestions that could mitigate these concerns.

I. BACKGROUND

While there is currently no comprehensive federal privacy law in the United States, there are several state data privacy laws and other sector-specific federal laws governing the collection of online information, including laws dealing with marketing, health information, and financial institutions.[11] Among these laws are (1) the Children's Online Privacy Protection Act (COPPA), which regulates the collection of information about individuals under the age of thirteen;[12] (2) the Health Insurance Portability and Accounting Act (HIPAA), which governs the collection of health information;[13] (3) the Fair Credit Reporting Act, which regulates credit information;[14] and (4) the Gramm-Leach-Bliley Act, which governs personal information collected by banks and other financial institutions[15]. The FTC is a crucial enforcer of these laws.[16] Empowered by the Federal Trade Commission Act, the FTC regulates commercial entities in an effort to prevent "unfair or deceptive acts or practices in or affecting commerce," seeks monetary relief on behalf of injured consumers, and conducts investigations related to commercial entities.[17]

Several states have also passed sectoral data privacy and information security laws.[18] However, only five states—California, Colorado, Connecticut, Utah, and Virginia—have enacted comprehensive data privacy laws as of November 2023.[19] The rise of state-level data privacy legislation is largely due to the federal government's failure to decide how to legislate on a broader, national scale.[20] Consumers, consumer advocates, and even commercial entities have pushed lawmakers to set a standard.[21]

11. Osano Staff, *Data Privacy Laws: What You Need to Know in 2023*, OSANO (Dec. 14, 2022), https://www.osano.com/articles/data-privacy-laws.

12. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06.

13. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d.

14. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2018).

15. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09, 6821–27.

16. Osano Staff, *supra* note 11.

17. Federal Trade Commission Act, 15 U.S.C. § 45; *see* 15 U.S.C. §§ 41–58.

18. An example of this is New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which enhanced New York's data breach notification law and established more stringent data security standards for businesses that collect data from New York residents. Osano Staff, *supra* note 11.

19. *Id.*

20. *Id.*

21. *Id.*

The California Consumer Privacy Act (CCPA), enacted on June 28, 2018, represents one of the most comprehensive state-level data privacy legislations.[22] It covers various sectors and includes vital definitions while outlining the rights of individual consumers.[23] It also imposes substantial duties on entities or individuals that collect personal information from California residents.[24] These responsibilities include the obligation to inform consumers about the categories of personal information collected or used, disclosing the purpose of that collection, and granting consumers the ability to access, correct, and delete such information.[25] This information must be disclosed in a privacy policy displayed on the collecting entity's website.[26] Furthermore, the CCPA safeguards the privacy rights of California consumers, including the right to know about the personal information a business collects about them and how it is used, the right to delete the collection, the right to opt out of the sale of their personal information, and the right to non-discrimination for exercising these rights.[27] The California Privacy Rights Act (CPRA), effective as of January 1, 2023, updates and expands upon this law.[28]

As of February 2024, 137 out of 194 countries worldwide have enacted data privacy and protection legislation.[29] The EU's GDPR set a global standard, as it is the most stringent law governing privacy and security globally and has served as a blueprint for numerous other countries' data protection laws.[30] It imposes obligations regarding the collection, security, sharing, and use of data obtained from EU residents.[31] Importantly, its jurisdiction extends to any entity that collects data from EU residents, regardless of the collecting entity's geographical location.[32]

22. *Id.*; *California Consumer Privacy* Laws, BLOOMBERG LAW, https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/#:~:text=The%20California%20Consumer%20Privacy%20Act%20(CCPA)%2C%20signed%20into%20law,1%2C%202020 (last visited Nov. 28, 2023).

23. Cal. Civ. Code §§ 1798.100–99 (2018).

24. *Id.*

25. *Id.* § 1798.100–05.

26. *Id.* § 1798.130.

27. *California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T. OF JUST. OFF. OF THE ATT'Y GEN. (May 10, 2023), https://oag.ca.gov/privacy/ccpa#sectionc.

28. Sam Pfeifle, *The Expert's Guide to California Data Privacy Law | CCPA & CPRA*, OSANO (Aug. 24, 2022), https://www.osano.com/articles/california-privacy-laws-ccpa-cpra.

29. *Data Protection and Privacy Legislation Worldwide*, UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited Feb 28, 2023).

30. Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Nov. 28, 2023); Regulation (EU) 2016/679, 2016 O.J. (L 119).

31. Regulation (EU) 2016/679, 2016 O.J. (L 119).

32. Wolford, *supra* note 30.

II. OVERVIEW OF THE AMERICAN DATA AND PRIVACY PROTECTION ACT

The ADPPA represents significant progress in the development of federal data privacy legislation, advancing further in the legislative process than any previous attempts.[33] While it shares several key components with other contemporary data privacy laws, such as the CCPA, the ADPPA also introduces distinctive features and differences that this Note will explore.

A. NOTABLE FEATURES OF THE ADPPA

The ADPPA extends its jurisdiction to encompass various industries and outlines specific terms and definitions that distinguish it from other privacy laws.[34] Notably, it broadens the scope by defining "covered entities" as "any entity or person that collects, processes, or transfers data and is subject to the FTC Act, is a common carrier under the Communications Act, or is a non-profit."[35] This is a very broad definition that covers most businesses and non-profits. Likewise, "covered data" is defined as "any information that identifies, is linked, or is reasonably linkable to an individual or a device," along with data or unique identifiers that can lead to such identification, like IP addresses and targeted advertising identifiers.[36] The ADPPA would essentially "prohibit covered entities from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by the individual or consumer unless the collection, use, or disclosure would fall under . . . [the] permissible purposes" outlined in the ADPPA.[37] Furthermore, the bill mandates that covered entities obtain "affirmative, express consent" from consumers before sharing their sensitive data with third parties.[38]

The ADPPA deviates slightly from other data privacy laws' definition of "children." In the ADPPA, "children" are defined as any individual under the age of seventeen, whereas most other data privacy laws define "children" as those under the age of thirteen or sixteen.[39] However, the ADPPA, like other laws, imposes specific requirements for the treatment of children's data.[40]

Additionally, the ADPPA introduces a broader concept of "sensitive data," including sixteen categories of data that go beyond the typical scope of sensitive data in other state privacy laws.[41] While many laws classify data

33. Davis, *supra* note 9.
34. JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (2022).
35. Davis, *supra* note 9.
36. *Id.*
37. GAFFNEY ET AL., *supra* note 34, at 2.
38. *Id.*
39. Davis, *supra* note 9.
40. *Id.*
41. *Id.*

such as race, ethnicity, genetic data, and children's data as sensitive, the ADPPA extends this classification to include information like device login credentials, and identifiers such as social security numbers.[42]

Another noteworthy feature of the ADPPA is that it will preempt all other data privacy laws at the state level.[43] For example, a California business currently subject to the CCPA would instead need to comply with the ADPPA. This aspect has raised substantial controversy, as many states prefer to retain control over their own data privacy legislation.[44] However, the ADPPA does make several exceptions to its preemption for more specific data privacy laws, allowing for the continuation of more specific data privacy laws like COPPA and specific elements of California's CPRA.[45]

Another significant component of the ADPPA is its inclusion of a private right of action, a provision not commonly found in most U.S. data privacy laws.[46] Under the ADPPA, individuals seeking to take legal action would need to first contact the FTC or their respective state's attorney general.[47] The FTC or state attorney general would then have sixty days to decide whether to intervene.[48] Furthermore, individuals must notify the entity they intend to sue and provide it with a forty-five-day window to rectify the violation before informing the FTC or state attorney general.[49]

The ADPPA also calls for the varying treatments of businesses based on the volume of data they handle, creating distinct categories for large data holders and small businesses.[50] Under the ADPPA, a large data holder is a business that generates over $250 million in gross annual revenue and processes the data of more than five million individuals or the sensitive data of 200,000 individuals annually.[51] This most likely applies to BigTech players such as Google and Meta.[52] Large data holders under the ADPPA are subject to additional disclosure, certification, and audit requirements.[53] Small businesses, on the other hand, are defined as businesses that (1) are not data brokers, (2) have less than $41 million in gross annual revenue, and (3) process the data of fewer than 200,000 individuals annually.[54] While most state data privacy laws typically do not impose restrictions on businesses handling data for fewer than 100,000 individuals, the ADPPA differs in its

42. *Id.*
43. *Id.*
44. *Id.*
45. Davis, *supra* note 9.
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. Davis, *supra* note 9.
52. *Id.*
53. *Id.*
54. *Id.*

approach.[55] Thus, virtually every business is subject to the ADPPA in some capacity.[56] While there are exceptions to what qualifies as a small business under the ADPPA, many businesses are likely to fall under its requirements.[57]

Additionally, the bill introduces a set of obligations for third-party data-collecting entities, including data brokers and businesses primarily reliant on processing and transferring data not directly acquired from consumers, such as Kochava.[58] These obligations include compliance with FTC auditing regulations and mandatory registration with the FTC when their data accumulation surpasses a specified threshold of devices and individuals.[59] The FTC would establish a publicly accessible registry of the third-party data collectors engaged in such activities.[60] Furthermore, the ADPPA introduces a provision granting data subjects the right to opt out of having their data collected by entities in the registry through a "Do Not Collect" choice.[61]

Lastly, one key feature of the ADPPA is consumers' right to opt out of data transfer.[62] This right is unique to the CPRA and empowers consumers to opt out of having their data transferred to third parties, including data brokers like Kochava.[63] Other state laws allow individuals to opt out of the sale of their data, but only the ADPPA and CPRA grant individuals the right to opt out of data transfers, regardless of whether or not a sale is involved.[64]

B. AMENDMENTS TO THE ADPPA

The features discussed above have been part of the bill since its introduction to Congress.[65] However, when the ADPPA passed the House of Representatives Committee on Energy and Commerce, it underwent several amendments aimed at increasing its chances of success in a vote in both the House and the Senate.[66] One significant point of contention is the bill's enforcement power.[67] Specifically, California representatives are opposed to the bill due to concerns that it would preempt the CPRA, leaving the state with a law that lacks the necessary enforcement authority.[68] Given California's considerable influence in the U.S. legislature, an amendment was introduced to designate the California Privacy Protection Authority (CPPA), the enforcement agency of the CPRA, as the agency responsible for

55. *Id.*
56. *Id.*
57. Davis, *supra* note 9.
58. *See* GAFFNEY ET AL., *supra* note 34, at 2.
59. *Id.*
60. *Id.*
61. *Id.*
62. Davis, *supra* note 9.
63. *See id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. Davis, *supra* note 9.

enforcing the ADPPA in the state.[69] For all other states, the enforcement of the ADPPA would fall under the jurisdiction of the FTC or the respective state's attorney general.[70]

Another amendment was made regarding the private right of action.[71] Originally, the bill allowed for a private right of action four years after enactment, but this amendment shortened the timeframe for individuals to sue entities for noncompliance to two years.[72] Furthermore, small businesses meeting specific criteria—such as generating less than $25 million in revenue annually, processing data of fewer individuals, and earning less than half their revenue from transferring covered data—would be exempt from private actions under the amended bill.[73]

Additional amendments were introduced to provide greater exclusions for employee data, further aligning the ADPPA with other privacy laws.[74] However, the bill broadened the scope of what constitutes employee data by including more data categories.[75] Another amendment was made to clarify the approach to children's data.[76] Under the ADPPA, entities are permitted to treat data differently only if they have "knowledge" that a consumer is under the age of seventeen.[77] This amendment introduced distinct definitions of what constitutes "knowledge" of a consumer's age, with variations based on the size of the business.[78] An additional amendment was made to grant legal authorization for the National Center for Missing and Exploited Children to access and work with children's data.[79] This amendment was justified because, without access to such data, the Center would be unable to effectively combat child abuse, abduction, and trafficking.[80]

III. IMPLICATIONS FOR BUSINESSES & CONSUMERS

The ADPPA has bipartisan support and the endorsement of several interest groups, including the Electronic Privacy Information Center and the Center for Democracy & Technology.[81] Forty-eight different public interest groups urged Congress to move the ADPPA forward, stating that the bill is a "meaningful compromise" and that failing to act may "forestall progress on this issue for years to come."[82] However, there are concerns among some

69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. Davis, *supra* note 9.
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. Davis, *supra* note 9.
81. GAFFNEY ET AL., *supra* note 34, at 4.
82. *Id.*

members of Congress and the general public about its potential impact on businesses and consumers.[83]

If the ADPPA is enacted, it will impose federal data privacy standards with which companies, including nonprofits and small businesses, must comply.[84] From a practical perspective, this could simplify compliance for businesses, as they would have a single federal standard to follow rather than navigating various statewide statutes.[85] What are some ways the ADPPA would impact business operations? Under the ADPPA, businesses must establish practices to protect covered data against unauthorized access and acquisition.[86] This concept, more commonly known as "privacy by design,"[87] would involve identifying and mitigating data privacy risks and providing evidence that adequate safeguarding practices are in place.[88] If necessary, businesses would also have to implement measures to ensure they collect and process data only in a manner deemed reasonably necessary by the permitted uses outlined in the ADPPA.[89] Additionally, businesses must make all privacy policies publicly available, and they would be prohibited from withholding services or products to individuals based on their choice to waive or exercise their privacy rights.[90] For businesses employing more than fifteen individuals, a data protection officer and a security officer must be appointed.[91] Large data holders would be required to furnish an annual metrics report, conduct yearly assessments on the impact of their systems, and submit these assessments to the FTC.[92] Lastly, businesses could be subject to civil lawsuits for violations of the law regarding the handling of consumers' personal data.[93]

One source of resistance to the ADPPA stems from the impact it would have on targeted advertising, which is the "economic driver of most

83. *Id.*

84. Hugo Loriot, *What the American Data and Privacy Protection Act Means for Marketers*, MKTG. DIVE (July 19, 2022), https://www.marketingdive.com/news/what-american-data-and-privacy-protection-act-means/626890/.

85. Osano Staff, *supra* note 11.

86. Lucas J. Schaetzel, *United States: Proposed Federal Data Protection Law Would Impose Duty of Loyalty and Allow Limited Private Right of Action*, MONDAQ (July 6, 2022), https://www.mondaq.com/unitedstates/privacy-protection/1209192/proposed-federal-data-protection-law-would-impose-duty-of-loyalty-and-allow-limited-private-right-of-action.

87. *Id.*

88. Loriot, *supra* note 85.

89. *10 Ways the American Data Privacy and Protection Act (ADPPA) Would Impact Your Business Operations*, TRŪATA (July 27, 2022), https://www.truata.com/articles/data-privacy-adppa-us-business-changes/ [hereinafter *10 Ways*].

90. Loriot, *supra* note 85.

91. *10 Ways*, *supra* note 90.

92. *Id.*

93. *Id.*

commercial surveillance in the first place."[94] While the bill does not outright ban targeted advertising, it does impose significantly stricter limitations on data collection for this purpose compared to other U.S. laws.[95] For example, it would completely prohibit targeting ads to minors and individuals based on their sensitive data.[96] This includes information identifying an individual's online activities over time and across online services and third-party websites.[97] In plain language, businesses would not be allowed to collect information about your online activities and utilize it for the purpose of marketing products or services to you.[98] This is a significant shift and targets one of the biggest issues in data privacy, especially given the evolution of advertising technology over the last few decades and the extensive personal information companies can now obtain.[99]

Under the amended version of the ADPPA, certain forms of targeted ads based on first-party data are allowed.[100] For example, if you shop for vacuums on Target.com, Target could still use that information to present vacuum-related ads on other websites.[101] However, Target is prohibited from amalgamating your shopping history with your broader online and mobile activities to deliver ads for unrelated products in which you never expressed interest.[102] Additionally, the bill places restrictions on large online platforms, such as Meta and Google, preventing them from deploying trackers on websites and apps for the purpose of data collection and profile-building for advertisers.[103]

In addition to these restrictions, the bill would require companies to provide users with the option to opt out of third-party data transfers.[104] However, it prohibits companies from using mechanisms to encourage users to click "Accept all cookies" and instructs the FTC to establish a standard for a universal opt-out, enabling users to decline all targeted advertising with a single click.[105] This feature of the ADPPA has encountered resistance from advertisers.[106] On July 20, 2022, the Association of National Advertisers issued a statement that opposed the bill because it would "prohibit companies from collecting and using basic demographic and online activity data for

94. Gilad Edelman, *Don't Look Now, but Congress Might Pass an Actually Good Privacy Bill*, WIRED (July 21, 2022, 8:00 AM), https://www.wired.com/story/american-data-privacy-protection-act-adppa/.
95. *Id.*
96. *Id.*
97. *Id.*
98. *See id.*
99. *Id.*
100. Edelman, *supra* note 95.
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*
106. *See* Edelman, *supra* note 95.

typical and responsible advertising purposes."[107] For consumers, this means more control over their data. Americans will have the right to access their personal data collected by ADPPA-covered entities, restrict certain uses of their data, and even have data deleted, with a timeframe of thirty to sixty days for ADPPA-covered entities to comply with such requests.[108] For marketers, this requires a thorough reevaluation of their existing procedures and perhaps an investment in technology geared toward ensuring privacy compliance.[109] The primary advantage for marketers lies in establishing a uniform framework that fosters consistency and predictability in achieving privacy compliance standards.[110]

IV. CRITIQUES & SUGGESTIONS

Despite receiving widespread support, the ADPPA still faces criticism for various reasons. One major concern is the lack of significant administrative enforcement power within the bill, with enforcement left to the FTC or state attorneys general.[111] This has led to concerns about the ability of these entities to enforce the law effectively, given their other priorities and the FTC's historical under-resourcing.[112] Another issue is the potential for the ADPPA to preempt state laws with different levels of enforcement and coverage, leading to concerns about the impact on states with more business-friendly data privacy laws.[113] Additionally, some have criticized the absence of a "duty of loyalty" requirement, which would obligate covered entities to act in their users' best interests when handling personal data.[114] However, there are potential solutions to address these concerns. One option involves establishing a dedicated data protection agency explicitly for ADPPA enforcement. Another approach is the inclusion of more specific provisions regarding state law preemption and the incorporation of a duty of loyalty.

107. *Id.*
108. *Id.*
109. Loriot, *supra* note 85.
110. *Id.*
111. Davis, *supra* note 9.
112. *Id.*; *Markup of the American Data Privacy and Protection Act: Hearing on H.R. 8152 Before the H. Comm. on Energy & Com.*, 117th Cong. 87 (2022), https://docs.house.gov/meetings/IF/IF00/20220720/115041/HMKP-117-IF00-Transcript-20220720.pdf#page=87 [hereinafter *Markup of American Data Privacy and Protection Act*].
113. Davis, *supra* note 9.
114. GAFFNEY ET AL., *supra* note 34, at 2; *see* Müge Fazlioglu, *Distilling the Essence of the American Data Privacy and Protection Act Discussion Draft*, THE INT'L ASS'N OF PRIV. PROS. (June 6, 2022), https://iapp.org/news/a/distilling-the-essence-of-the-american-data-privacy-and-protection-act-discussion-draft/.

A. ADMINISTRATIVE ENFORCEMENT

One of the biggest criticisms the ADPPA has received is the lack of significant administrative enforcement.[115] While the bill does provide for civil enforcement via its private right of action, it lacks substantial administrative enforcement capabilities.[116] The GDPR, for example, has dedicated data protection authorities responsible for enforcing the law and penalizing non-compliant entities.[117] In California, the CPPA serves the singular purpose of safeguarding consumers from the misuse of their personal data by businesses that collect it.[118] The CPPA possesses the authority to levy fines, promulgate regulations, and conduct business audits.[119] Under the ADPPA, however, enforcement power is delegated to either the FTC or state attorneys general, both of which have priorities that rank higher than data protection enforcement.[120] Additionally, the FTC is historically under-resourced.[121] Senator Maria Cantwell, a Washington Democrat and Chair of the U.S. Senate Committee on Commerce, Science, and Transportation, has been a prominent critic of the bill.[122] Cantwell has expressed that she cannot support the bill "unless House lawmakers add tougher enforcement measures, including limits on forced arbitration and a broad right for individuals to sue companies that violate the law."[123]

One possible solution to this issue would be creating a dedicated data protection agency with the sole purpose of enforcing the ADPPA, similar to the CPPA's responsibilities in California. The United States is one of the few countries in the world that does not have a federal data protection agency and is the only member of the Organisation for Economic Co-operation and Development without one.[124] Many interest groups, such as the Electronic Privacy Information Center (EPIC), have long expressed this urgent need for a data protection agency.[125] "Virtually every other advanced economy has recognized the need for an independent agency to address the challenges of the digital age. . . . As the data breach epidemic reaches unprecedented

115. Davis, *supra* note 9.
116. *Id.*
117. *Id.*
118. *See About CPPA*, CA.GOV, https://cppa.ca.gov/about_us/ (last visited Nov. 28, 2023); *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 86.
119. *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 86.
120. Davis, *supra* note 9.
121. *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 87.
122. Orion Donovan-Smith, *McMorris Rodgers, House Democrats Back Compromise to Pass Historic Privacy Bill. But Will Cantwell Let It Pass?*, THE SPOKESMAN-REVIEW (July 25, 2022), https://www.spokesman.com/stories/2022/jul/25/historic-data-privacy-law-could-be-within-reach-if/?utm_campaign=wp_the_technology_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_technology202.
123. *Id.*
124. *The U.S. Urgently Needs a Data Protection Agency*, ELEC. PRIV. INFO. CTR., https://epic.org/campaigns/dpa/ (last visited Nov. 28, 2023).
125. *See id.*

levels, the need for an effective, independent data protection agency has never been greater."[126]

Establishing an independent agency focused solely on data privacy and protection would enable more effective utilization of resources for monitoring the use of consumers' personal information.[127] This agency would be staffed with people who "possess the requisite expertise to regulate the field of data security."[128] This would solve the issue of the FTC being under-resourced and too preoccupied with other concerns. According to EPIC, a data protection agency would "safeguard the personal data of individuals," prevent and reduce discrimination and other negative impacts resulting from data processing, and limit the use, collection, and sharing of this data.[129] It would also "oversee high-risk data practices," ensuring that companies process data in "fair, just, non-deceptive, and non-discriminatory" ways.[130] The agency would also investigate the ethical, social, economic, and civil rights impacts of data collection practices and propose remedies and policies to improve these practices.[131] Lastly, it would "promulgate rules to protect the privacy and security of personal data."[132]

B. STATE LAW PREEMPTION

One of the most significant points of contention revolves around the ADPPA's preemption of other state laws, which vary in enforcement and coverage.[133] The interaction between a federal privacy standard and a growing number of state laws has been a central topic of discussion in Congress.[134] The ADPPA would essentially preempt state data privacy laws that are more business-friendly.[135] The Attorney General of California, along with nine other state attorneys general, sent Congress a letter criticizing the ADPPA because it would set a "ceiling" for privacy rights rather than a "floor."[136] In their view, states should retain the authority to enact their own privacy laws, allowing them to "legislate responsively" in response to evolving technology and practices.[137] There is "strong precedent for federal

126. *Id.*
127. *See id.*
128. *Id.*
129. *Id.*
130. *The U.S. Urgently Needs a Data Protection Agency*, *supra* note 125.
131. *Id.*
132. *Id.*
133. Davis, *supra* note 9.
134. Cristiano Lima, *Federal Privacy Bill trumps California's Law, Advocates Say*, WASH. POST (July 15, 2022), https://www.washingtonpost.com/politics/2022/07/15/federal-privacy-bill-trumps-californias-law-advocates-say/.
135. Davis, *supra* note 9.
136. ROB BONTA, LETTER TO CONGRESS RE FEDERAL PRIVACY, at 3 (July 19, 2022), https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20re%20Federal%20Privacy.pdf.
137. *See id.*; GAFFNEY ET AL., *supra* note 34.

privacy laws to serve as a floor but not a ceiling."[138] For example, every individual in the United States benefits from HIPAA medical privacy protections, but states have implemented additional, more stringent laws to address specific needs and respond more promptly than Congress to emerging issues in healthcare privacy.[139]

During the Commerce Committee's July 20 markup of the ADPPA, some members voiced similar concerns regarding the preemption of state laws.[140] One example used to support their concerns is that HIPAA does not override state laws that grant individuals expanded rights to their health information.[141] They also gave recognition to the Supreme Court's June 2022 decision in *Dobbs v. Jackson Women's Health Organization*, which opened the door to some states criminalizing abortion, and expressed that the ADPPA has a major loophole that could allow law enforcement to access private data to target women.[142] For example, a prosecutor in a state that criminalizes abortion could use the bill against women by using their private, sensitive data from sources such as search histories or reproductive health apps like Flo.[143]

Another argument raised in the debate over state law preemption pertains to the potential consequences for California agencies tasked with enforcing data privacy laws.[144] Critics argue that the ADPPA could create ambiguity regarding these agencies' authority to protect California's constitutional right to privacy.[145] State law preemption would also place major enforcement responsibilities on the FTC, which, again, may strain the agency's capacity and consume valuable resources.[146] Additionally, the CPPA expressed concerns to former House Speaker Nancy Pelosi that "the bill would hurt Californians by limiting state legislators and regulators from" providing more protections to its residents.[147] Other states have joined in with their concerns, expressing that the ADPPA would render recent additions to their laws useless. For example, Illinois has the Biometric Information Privacy Act, enacted in 2008, which serves as a benchmark for laws addressing biometric

138. Hayley Tsukayama, *Federal Preemption of State Privacy Law Hurts Everyone*, ELEC. FRONTIER FOUND. (July 28, 2022), https://www.eff.org/deeplinks/2022/07/federal-preemption-state-privacy-law-hurts-everyone.

139. *Id.*

140. *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 85, 91–92.

141. *Id.* at 85.

142. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022); *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 86.

143. *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 86; *see* Fertility-Tracking App Press Release, *supra* note 5 and accompanying text (discussing Flo as a menstrual period and fertility tracking app).

144. *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 86.

145. *Id.* at 86–87.

146. *Id.* at 87.

147. Lima, *supra* note 135 (internal quotation marks omitted).

privacy.[148] Many other states passed similar or identical legislation to protect their own constituents.[149] While Illinois's law would remain in effect under the ADPPA's preemption, other states and cities would be prevented from maintaining or enacting similar laws.[150]

Other Congressional members and commentators have pushed back on these criticisms, pointing to the strengths of the ADPPA's protections and the importance of setting a federal data privacy standard.[151] They argue that without a federal standard, states might contend that their laws provide stronger protections, potentially leading to protracted legal disputes.[152] Some have also argued that states with privacy laws already in place should not obstruct federal legislation to preserve their own laws at the expense of rights and protections for residents across the United States.[153] States that do not currently have data privacy laws would benefit from "a federal baseline."[154]

One proposed solution is the introduction of a sunset provision for preemption aimed at addressing concerns regarding state-level intervention.[155] This provision would establish a specific timeframe after which state regulators could promulgate privacy rules that offer stronger protection than the federal law.[156] Nevertheless, Congress would have to decide the time period of this sunset, which could be another contentious point of debate.[157] However, even this suggestion has brought opposition. Representative Collin Walke, a member of the Oklahoma House of Representatives, argues that policymakers should choose between two options: maintaining a network of state laws where certain states retain their regulatory powers and can address matters on their own schedule or implementing full federal preemption.[158] Walke believes that granting states this time to create "consistency and homogeneity" would only "create balkanization down the road" and that "the better route would be to set a federal floor, not a ceiling."[159]

148. *See* Biometric Information Privacy Act 740 ILCS 14 *et seq.* (2008); Tsukayama, *supra* note 139.
149. *Id.*
150. *Id.*
151. *Markup of American Data Privacy and Protection Act*, *supra* note 113, at 173.
152. *Id.*
153. Joseph Duball, *State Views on Proposed ADPPA Preemption Come into Focus*, THE INT'L ASS'N OF PRIV. PROS. (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/.
154. Tsukayama, *supra* note 139.
155. Duball, *supra* note 154.
156. *Id.*
157. *See id.*
158. *Id.*
159. *Id.*

C. FAILURE TO IMPOSE A "DUTY OF LOYALTY"

Another concern that members of Congress and other commentators have raised is the "bill's failure to impose a duty of loyalty on covered entities."[160] The duty of loyalty under the ADPPA focuses on data minimization, requiring covered entities to collect and process covered data in a manner that is "reasonably necessary and proportionate to the product or service being provided."[161] Furthermore, the ADPPA imposes prohibitions or limitations on certain actions related to covered data, such as transferring or sharing specific covered data, including social security numbers, passwords, biometric information, and genetic information.[162] The extent to which the ADPPA's duty of loyalty is enforced on a covered entity hinges on various factors, such as "(1) its size and complexity; (2) sensitivity of the covered data at issue; (3) volume of covered data at issue; (4) number of individuals that the covered entity collects covered data from and (5) the costs of implementing security and risk mitigation measures."[163]

The requirements in the "Duty Of Loyalty" provision differ from those included in the Consumer Online Privacy Rights Act (COPRA) or the Data Care Act.[164] For example, COPRA's duty of loyalty prohibits businesses from engaging in "harmful" data practices, which the ADPPA defines as "using covered data in a manner that causes or is likely to cause injury" to the data subject.[165] In addition, the Data Care Act's duty of loyalty prohibits covered providers from utilizing data in a manner that would "benefit the provider to the detriment of the end user" and "would result in reasonably foreseeable and material physical harm or be unexpected and highly offensive to the end user."[166] As previously discussed, the ADPPA's "Duty of Loyalty" provision imposes a requirement to minimize consumer data and categorizes specific prohibited data practices, but it does not have a broad restriction on providers from engaging in actions that could potentially harm individuals.[167] While the ADPPA has "loyalty duties," it does not "explicitly obligate companies to act in the best interests of people exposing their data or prohibit them from designing digital tools and processing data in a way that conflicts with trusting parties' best interests."[168]

160. GAFFNEY ET AL., *supra* note 34, at 4 (internal quotation marks omitted).

161. Lucas J. Schaetzel, *United States: Proposed Federal Data Protection Law Would Impose Duty of Loyalty and Allow Limited Private Right of Action*, MONDAQ (July 6, 2022), https://www.mondaq.com/unitedstates/privacy-protection/1209192/proposed-federal-data-protection-law-would-impose-duty-of-loyalty-and-allow-limited-private-right-of-action.

162. *Id.*

163. *Id.*

164. The Consumer Online Privacy Rights Act (COPRA) and the Data Care Act are past consumer privacy bills that were introduced in the 117th Congress. GAFFNEY ET AL., *supra* note 34, at 4.

165. *Id.* (internal quotation marks omitted).

166. *Id.* at 5 (internal quotation marks omitted).

167. *Id.*

168. Fazlioglu, *supra* note 115 (internal quotation marks omitted).

Thus, there must be more extensive discussions by lawmakers regarding what the ADPPA's "duty of loyalty" should encompass.[169] A decision must be reached on whether the duty of loyalty, as the ADPPA implies, is synonymous with restrictions on the processing of sensitive personal information, privacy by design, and data minimization, or rather, if it is a principle intended to prevent entities from making decisions out of self-interest that are harmful to individuals whose data they collect and use, as the COPRA and Data Care Act assumes it to be.[170]

CONCLUSION

In this digital age, individuals are frequently required to provide personal information for various purposes, ranging from online purchases to healthcare.[171] It is crucial that businesses and entities be held accountable for protecting the personal information they have been entrusted with and using it only for specified purposes.[172] Establishing a federal standard would ensure consistent protection of individuals' data privacy and security across the United States, regardless of their location. So, what is next for the ADPPA? As of today, the ADPPA has successfully advanced through the House committee, where it received amendments on July 20, 2022, as described above.[173] Next, the bill must pass a vote in the House.[174] If it passes, the bill will proceed to the Senate, where it will be introduced and referred to the Senate Committee on Commerce, Science, and Transportation for thorough examination.[175] Upon receiving approval from the Committee, the bill will advance to the Senate floor for a formal vote and subsequently make its way to President Biden's desk for final approval.[176]

One of the major challenges facing the bill is opposition from Senator Cantwell, chair of the Senate Committee on Commerce, Science, and Transportation.[177] Senator Cantwell will play a key role in the study of the bill before it is introduced to the Senate.[178] Additionally, any proposed amendments to the bill that seek to enhance enforcement measures could potentially jeopardize its bipartisan support, thus significantly impacting its chances of becoming law.[179] It is exciting that there is bipartisan and bicameral consensus on the necessity of a federal privacy law to safeguard citizens. However, the combination of objections from California and lack of

169. *Id.*
170. *Id.*
171. Davis, *supra* note 9.
172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*
176. *Id.*
177. Davis, *supra* note 9.
178. *Id.*
179. *Id.*

support from a key Senator presents formidable challenges to the ADPPA's enactment.[180] Although this bill has made substantial progress compared to previous federal data privacy bills, it still faces a lengthy journey before it becomes law and may undergo significant revisions along the way.[181]

Erin J. An[*]

180. Emily Catron & Gary Kibel, *Federal Data Privacy Legislation: Differences with State Laws Raise Preemption Issues*, REUTERS (Aug. 10, 2022, 10:19 AM), https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10/.

181. Davis, *supra* note 9.

* J.D. Candidate, Brooklyn Law School, 2024; B.S. in Management, Concentration in Marketing, Boston College, 2021. My heartfelt gratitude to the *Brooklyn Journal of Corporate, Financial & Commercial Law* editors and staff for their dedicated efforts in bringing this publication to life. Thank you to my parents, Kim and Rick, and my siblings, Swan, Eric, and Justin, for always supporting me throughout my law school and professional journey. Finally, special thank you to my friends for their continued love, encouragement, and support.