PROTECTING DATA IN THE DIGITAL AGE: A CALL FOR FEDERAL PRIVACY PROTECTION

By Anastasia Del Roio[1]
Edited by Remi Bass

In the postmodern digital age, there is no federal statute to protect consumer data privacy. Although federal statutes such as the Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA) protect specific areas of consumer data, a comprehensive data privacy statute must be implemented to prevent corporations from using and selling consumer data without consent. The California Consumer Privacy Act (CCPA) is a prime example of an all-encompassing data privacy statute; it holds businesses accountable for the unconstitutional use of consumer data by requiring them to inform consumers of their intentions and ask for consent to use consumer data. Attempts to enact a comprehensive federal statute via the American Data Privacy and Protection Act (ADPPA) and the American Privacy Rights Act (APRA) have been largely unsuccessful, as the ADPPA died in the House of Representatives in 2022, and the future of the APRA remains uncertain. Though the APRA ameliorates the past concern of state law preemption, the act has been languishing in committee since its introduction in 2024. Ultimately, a well-constructed comprehensive statute uses effective elements of the CCPA to set a baseline of privacy protections while addressing preemption concerns raised by previous legislative attempts. This Note discusses each of these documents and poses how a successful comprehensive federal statute may be formed.

[1] B.A. Candidate for Political Economy (major) and French (minor), Tulane University School of Liberal Arts, Class of 2027. B.S.M. Candidate for Legal Studies in Business (major), A.B. Freeman School of Business, Class of 2027.

I. Introduction

The consequences of failing to protect consumer data privacy span far beyond what many Americans may suspect. When corporations collect consumer data, they can use it to spam individuals with unsolicited advertisements, predict and influence consumer behavior, or sell this information for profit.[2] Corporations' sale of personal data often happens without consumer consent or knowledge of what they are disclosing.[3] The non-consensual purchase of data can affect consumers' personal and professional lives by leading to discrimination if sensitive information is sold.[4] Furthermore, data breaches, the exposure of personal records, phishing scams, identity theft, and other consumer harms are more likely to occur when data sale and use go unregulated.[5] In response to these modern threats, 20 states—including California—have enacted comprehensive consumer privacy laws. California's law, the California Consumer Privacy Act (CCPA), exemplifies this trend with its holistic approach to protecting consumer data.[6] However, despite efforts at the state level and multiple federal attempts, no comprehensive federal privacy law currently exists. On the federal level, statutes protecting narrow areas of consumer data privacy are in place, such as the Children's Online Privacy Protection Act (COPPA); that said, this act only protects the data of children under the age of 13.[7] Other federal statutes, such as the Electronic Communications Privacy Act (ECPA) and the Health Insurance Portability and Accountability Act (HIPAA), protect online correspondence and personal records, but there are gaps when it comes to general online activity and personal information disclosed to businesses.[8]

This Note begins by examining the CCPA and its strengths in protecting consumer privacy. It then explores federal attempts to create a comprehensive statute, focusing on the failed ADPPA and the newly proposed APRA. This Note will conclude by discussing how the strong suits of the CCPA can be applied to cultivate a successful comprehensive federal statute and end by emphasizing the importance of consumer data privacy protection. It is important to emphasize that this Note will not recommend revisions to the APRA specifically, but rather discuss the CCPA's strong suits and how they can be used to craft a new federal statute. While there have been attempts at a comprehensive consumer data privacy statute in the past, they have largely been shot down due to concerns about preemption of state laws. This Note will discuss how these can be resolved in a successful statute.

[2] "Consumer Data: Increasing Use Poses Risks to Privacy." U.S. Government Accountability Office, September 13, 2022. https://www.gao.gov/products/gao-22-106096.
[3] Id.
[4] Id.
[5] Id.
[6] "Which States Have Consumer Data Privacy Laws?" Bloomberg Law, December 23, 2024. https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker
[7] Children's Online Privacy Protection Act, 15 U.S.C. 6501-6505, §312 (1998).
[8] "Consumer Data Privacy Laws." Bloomberg Law, January 3, 2025. https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-laws/.

Currently, consumer data privacy rights are only holistically protected in states that have enacted comprehensive statutes. This means that in over half of the United States, citizens' data privacy is not statutorily protected. When exploited, personal information collected by businesses can result in discrimination, identity theft, and fraud. To ensure that all Americans' rights are protected, Congress should enact a comprehensive federal data privacy statute that sets a national baseline of consumer protections—drawing upon the California Consumer Privacy Act—while preserving states' ability to implement stronger safeguards, thereby avoiding the preemption pitfalls of past legislation and respecting the constitutional balance between federal authority and state sovereignty.

II. Overview of the California Consumer Privacy Act

The first section of the CCPA is entitled "General Duties of Businesses that Collect Personal Information."[9] Notably, this section requires businesses to disclose the following three facts to consumers: the type of information collected, why it is collected, and whether or not this information will be "sold or shared."[10] When businesses act as a third party for data sales, they must display information on their website homepage detailing their purpose for collecting the data and intent to sell it.[11] Lastly, and uniquely, the "collection, use, retention, and sharing" of a consumer's personal information is required by law to be "reasonably necessary and proportionate to achieve the purposes" for which the personal information was originally collected.[12]

Next, the CCPA outlines "Consumers' Right to Delete Personal Information."[13] As is implied, this section grants consumers the right to request that a business delete any collected personal information and requires that businesses uphold these rights upon request.[14] It is also necessary that a business disclose these rights to consumers before any data collection.[15] The following two sections outline "Consumers' Right to Correct Inaccurate Personal Information" and "Consumers' Right to Know What Personal Information is Being Collected."[16] This means that consumers are entitled to correct any information they hold to be inaccurate.[17] Likewise, the consumer has a right to request that a business disclose what personal information they are collecting and request access to this information at any time.[18]

The final sections of the CCPA outline additional consumer rights important to data protection. Firstly, consumers have the right to know what information will be sold or shared and

[9] California Consumer Privacy Act, 1798.100 - 1798.199.100, §1798.100(a), (2018).
[10] Id.
[11] Id. at §1798.100(b)
[12] Id. at §1798.100(c)
[13] Id. at §1798.105
[14] Id.
[15] Id.
[16] Id. at §1798.105-1798.110
[17] Id. at §1798.106
[18] Id. at §1798.110

to whom it will be sold or shared.[19] One of the most important and groundbreaking aspects of the CCPA is the right for consumers to opt out of the "sale or sharing of personal information."[20] This right can be exercised at any time, such that if they initially fail to opt out, they can choose to opt out later on.[21] A consumer can also limit the use of their information by a business at any time. A unique aspect of the CCPA is that it imposes certain "notice, disclosure, correction, and deletion requirements" on businesses.[22] The most notable of these requirements is that all of the information a business needs to disclose must be presented to consumers in a "reasonably accessible form."[23]

A. The People v. DoorDash (2024)

One of the most prominent cases involving the California Consumer Privacy Act is *The People v. DoorDash* (2024). This case involved a judgment against DoorDash for violations of the CCPA due to their failure (1) to inform users that their information would be sold and (2) to uphold users' right to opt out.[24] DoorDash sold consumer information to marketing co-ops, despite their privacy policy never mentioning this.[25] The purpose of purchasing this information by the marketing co-ops was to strategically target consumers with unsolicited advertisements. The advertisements were curated uniquely for consumers using the information purchased from DoorDash without consumers' consent.[26]

It was ultimately ruled by the Superior Court of the State of California in San Francisco that DoorDash would have to pay a $375,000 judgment to the Attorney General of California for violations of the CCPA for selling consumers' personal information "without providing notice or an opportunity to opt out" and for failure to disclose to consumers that their personal information would be sold and to which business entities this would occur.[27] They were also required to perform certain injunctive measures, including complying with the CCPA for the indefinite future, reviewing their contracts with the marketing co-ops to comply with CCPA regulations, and providing annual reports to the California Attorney General.[28] The judgment was issued by Judge Ulmer in February 2024 and is just one of many monumental cases in California that resulted from national corporations violating the CCPA.[29]

III. Attempts at Federal Legislation

[19] Id. at §1798.115
[20] Id. at §1798.120
[21] Id.
[22] Id. at §1798.120
[23] Id. at §1798.121
[24] *The People v. DoorDash (2024)*, CGC-24-612520 (Cal. 2024).
[25] Id.
[26] Id.
[27] Id.
[28] Id.
[29] Id.

While 20 states in the United States have enacted comprehensive consumer data privacy statutes, federal efforts to implement one have yet to succeed. There have been two attempts toward implementation: one has failed, and the other is stalled in committee as of May 2025.[30] The first attempt was the American Data Privacy and Protection Act, which passed in the House Energy and Commerce Committee in 2022 with bipartisan support but died after failing to advance to the House of Representatives floor.[31] The second attempt was the American Privacy Rights Act. The APRA was introduced in 2024 and passed successfully through the House Energy and Commerce Subcommittee on Data, Innovation, and Commerce in June 2024.[32] The APRA currently awaits a full committee vote, which will determine whether or not it will move forward to the House of Representatives floor.[33] This section will break down the elements of both acts, noting which are strong and which led to failure.

A. American Data Privacy and Protection Act

The American Data Privacy and Protection Act was designed to regulate how businesses could collect, use, and handle consumers' personal information.[34] It required companies to "limit the collection, processing, and transfer of personal data to that which is reasonably necessary to provide a requested product or service."[35] Essentially, companies were permitted to only collect data for their relevant and expressed purposes and were prohibited from using consumer data beyond these purposes.[36] Moreover, the bill forbade companies from transferring individuals' data without their expressed consent.[37]

In regard to consumer rights, the bill empowered consumers with the "right to access, correct, and delete personal data."[38] Likewise, consumers were given the right to opt out if a business was collecting data to engage in targeted advertising.[39] Building upon COPPA, the bill expanded protections for minors to include individuals under the age of 18 rather than solely 13 and under.[40] This would have, in turn, required parents to give express consent for the collection of "covered minor[s']" data.[41] Importantly, the ADPPA would have prevented collected data from being used for discriminatory purposes, primarily based on "race, color, religion, national

[30] Niemiec, Sarah G. "Understanding Data Privacy Protections: ADPPA and APRA." The Alliance for Citizen Engagement, March 15, 2025. https://ace-usa.org/blog/research/research-technology/understanding-data-privacy-protections-adppa-and-apra/.
[31] American Data Privacy and Protection Act, H.R.8152, 117th Cong. (2021).
[32] American Privacy Rights Act, H.R.8818, 118th Cong. (2024).
[33] Niemiec, Sarah G. "Understanding Data Privacy Protections: ADPPA and APRA." The Alliance for Citizen Engagement, March 15, 2025. https://ace-usa.org/blog/research/research-technology/understanding-data-privacy-protections-adppa-and-apra/.
[34] American Data Privacy and Protection Act, H.R.8152, 117th Cong. (2021).
[35] Id.
[36] Id. at § 101(b)
[37] Id.
[38] Id. at § 202
[39] Id.
[40] Id. at § 205
[41] Id.

origin, sex, or disability."[42] Had the bill passed, the Federal Trade Commission would have been entrusted with enforcing these regulations to prevent consumer harm resulting from fraud, identity theft, discrimination, and other potential harmful consequences of data collection.[43]

Though these elements of the ADPPA are undeniably positive, the element that ultimately led to the bill's demise was the condition that it "preempts state laws that are covered by the provisions of the bill" with a few express exceptions.[44] If the ADPPA were to pass, it would have nullified pre-existing state laws such as the CCPA. However, the ADPPA did not include the niche provisions and regional specifications that state laws had. Thus, the ADPPA's preemption clause concerned lawmakers from states that had already implemented comprehensive data privacy statutes, as they did not want a federal law to render their statutes void.[45] Considering that it was primarily the democratic states with robust pre-existing statutes, the House Democrats ended up accounting for the majority of opposition to the bill.[46] From California's perspective, for instance, opposing the bill arguably *protected* consumers' data privacy rights, as the California Consumer Privacy Act ultimately had stronger provisions than the federal bill.

B. American Privacy Rights Act

Although the American Privacy Rights Act is similar to the American Data Privacy and Protection Act in terms of subject area, the APRA's scope is substantially wider. Like the ADPPA, it affords consumers the right to access, correct, and delete data a business may obtain from them.[47] Concerning its usage regulations, it mirrors the ADPPA in requiring businesses to allow consumers to opt out of personal data usage and effectively limits businesses' data usage.[48] The significant differences between these bills, however, must also be examined, considering that the alterations made from the ADPPA to the APRA have garnered more bipartisan support for the APRA while also sparking contempt.

Most notably, the APRA widens the definition of personal data to protect a larger scope of consumer data than the ADPPA.[49] While the ADPPA primarily accounted for the protection of personal information a user input into a website, the APRA protects additional data, such as a user's online activity that may have been taken note of and retained by businesses' websites. Moreover, the APRA has stricter consent requirements, stipulating that, in most scenarios, a company must ask a consumer for explicit consent to retain, use, or sell their data.[50] The ADPPA, on the other hand, allowed for implied consent to suffice in most instances. Another one of the

[42] Id. at § 207(a)
[43] Id. at § 207(b)
[44] American Data Privacy and Protection Act, H.R.8152, 117th Cong. (2021).
[45] Klosowski, Thorin. "The State of Consumer Data Privacy Laws in the US (And Why It Matters)." The New York Times, September 6, 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
[46] Id.
[47] American Privacy Rights Act, H.R.8818, 118th Cong. (2024).
[48] Id. at § 102
[49] Id. at § 101
[50] Id. at § 105

APRA's advantageous features is the right it gives consumers to sue companies directly for privacy violations.[51] While a consumer may have been able to achieve this under the ADPPA, this provision is explicitly outlined in the APRA.

Presumably, the most important difference in the APRA is its stance toward the preemption of state laws. To avoid disrupting strong data privacy protection laws already established by certain states, the APRA ameliorates this concern by allowing the statute to coexist with state statutes, rather than preempting them.[52] This modification has substantially increased the level of bipartisan approval of the APRA as compared to the ADPPA. Two other fundamental differences to note are the explicit exemptions from regulations sometimes granted to small businesses and the slightly fewer provisions for the protection of minors compared to those included in the ADPPA. In light of these differences, many critics argue that the APRA is not a perfect example of a comprehensive federal data protection statute.[53] Nonetheless, it constitutes a significant advancement from the ADPPA in that it allows state laws to coexist with it.

IV. Establishing the Baseline and Overcoming Preemption

Despite the several shortcomings of past attempts toward a comprehensive federal data privacy statute, each setback revealed pivotal concerns that must be accounted for going forward. One can learn from the American Data Privacy and Protection Act that for a comprehensive data privacy statute to be successful at the federal level, it cannot preempt state laws. This provision of the ADPPA was what ultimately led to its demise, as federal lawmakers were hesitant to allow a weaker federal statute to overrule all the provisions put in place by stronger existing state statutes.[54] While the American Privacy Rights Act has not yet been voted on outside of the subcommittee in the House of Representatives, it is evident that a majority of lawmakers' hesitations stem from the weaker provisions it provides in some areas, such as its reduced protection for minors compared to the ADPPA's protections.[55] There are also remaining preemptive concerns due to the APRA's narrow wording, specifically concerning small businesses.[56] Through this debate, it becomes clear that lawmakers from states *without* a pre-existing comprehensive statute desire a broader act that encompasses a wide range of issues, whereas lawmakers from states *with* pre-existing statutes want a statute that remains narrow enough in scope to not preempt state laws. One solution to this would be to model the federal statute after a strong and successful existing state statute, such as the California Consumer

[51] Id. at § 107
[52] Id. at § 116
[53] C. Linebaugh et al., "The American Privacy Rights Act," Congressional Research Service, https://crsreports.congress.gov/product/pdf/LSB/LSB11161.
[54] Mahoney, Maureen. Legislative Update and Authorizing CPPA's Position on Pending Legislation, p. 3, May 10, 2024. https://cppa.ca.gov/meetings/materials/20240510_item3_profiling_legislation.pdf.
[55] Id.
[56] Benson, Peter J, et al., Summary of the American Privacy Rights Act, May 31, 2024. https://www.congress.gov/crs-product/LSB11161.

Privacy Act, to set a clear federal baseline for consumer privacy rights. From there, states would be able to craft their own statutes to provide specialized, regional data privacy protection to consumers and thereby ameliorate the preemptive concerns of the ADPPA.

A. Federal Application of the California Consumer Privacy Act

The CCPA was passed in 2018 and is widely known as the first state comprehensive data privacy statute to be enacted in the United States.[57] As a result, the CCPA set a precedent for comprehensive statutes in other states that would be passed in the following years,[58] including those in Colorado, Iowa, Utah, Virginia, and Connecticut. With the CCPA serving as a trailblazing piece of legislation in the digital age, these states used the Act as a base for their statutes, adjusting certain aspects to account for regional differences.[59] Given its history, the California Consumer Privacy Act is the ideal state statute to model a federal statute after. Our understanding of comprehensive consumer privacy statutes originates from the CCPA, and it has had a successful track record, as observed in cases such as *The People v. DoorDash*. Modeling a federal statute after the CCPA's exemplary elements will mediate the issues encountered in previous federal statute attempts and be effective in delegating and protecting citizens' rights.

To create a robust, comprehensive federal statute, it's imperative to draw upon the CCPA's strongest elements, including its explicit outlining of consumer rights, the right to non-discrimination for exercising one's rights, and effective enforcement policies to hold companies accountable.

The consumer rights clearly outlined in the CCPA are as follows: the right to know what personal information a business collects and how it is used and shared; the right to delete collected personal information; the right to opt-out of the sale or sharing of personal information; the right to correct inaccurate personal information; and the right to limit the use and disclosure of sensitive personal information collected.[60] Ensuring that all citizens in America have these rights is crucial to having an effective, just statute.

Next, consumers' right to non-discrimination for exercising their rights is essential. Since one of the primary aims of a comprehensive data privacy statute is to safeguard consumers' data from being used for discriminatory purposes by corporations, ensuring that consumers are explicitly granted the right to non-discrimination will strengthen the statute's equitability. Under the CCPA, companies are required to grant consumers' requests to view, edit, or delete any obtained data and are prohibited from treating consumers differently for making these requests.[61]

[57] "California Consumer Privacy Laws – CCPA & CPRA." Bloomberg Law, January 3, 2025. https://pro.bloomberglaw.com/insights/privacy/california-consumer-privacy-laws/.
[58] Id.
[59] "Which States Have Consumer Data Privacy Laws?" Bloomberg Law, December 23, 2024. https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/.
[60] California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General, January 28, 2025. https://oag.ca.gov/privacy/ccpa.
[61] California Consumer Privacy Act, 1798.100 - 1798.199.100, §1798.100(a), (2018).

This provision will prevent substantial injuries to consumers and prevent the need for litigation in many scenarios.

Lastly, provisions for effective enforcement of the statute are necessary to ensure the federal statute's success. Strict adherence to the CCPA is widely enforced by the California Attorney General and the California Department of Justice.[62] Penalties for violators of the CCPA are high and can include hefty fines and injunctive measures.[63] *The People v. DoorDash* case was an instance where the California Attorney General took considerable action against DoorDash for violating the CCPA, requiring the company to pay $375,000 in fines and complete injunctive measures, such as reports to the Attorney General and amending their privacy policy to comply with CCPA regulations.[64] Similarly, both the ADPPA and APRA include provisions that authorize the Federal Trade Commission to penalize violators of the federal statute.[65] Emulating the CCPA's enforcement policies in the federal statute guarantees that violators will be held accountable, thus enhancing the statute's effectiveness and credibility.

B. Solving the Preemption Concern

Once a statute is crafted based on the principles of the CCPA, the question of preempting state laws remains unresolved. Similar to the APRA, a successful comprehensive federal statute should specifically outline that the statute shall not preempt state law. Ideally, the statute will serve as a nationwide baseline that individual states can build on and specialize to suit regional needs. By modeling the federal statute after the CCPA, which was the first comprehensive statute on which others are based, the federal statute will be strategic enough to avoid diluting state statutes in areas where it may preempt them. Strengthening the provisions of the comprehensive federal statutes beyond what was done in previous attempts, specifically mirroring the state statute that served as the model for other state statutes, will garner a higher level of support for the statute and lead to its success in both becoming law and guaranteeing Americans' data privacy rights.

Preemption remains a substantive concern when considering how best to enact a comprehensive federal statute. If a federal statute were to explicitly preempt state laws, states would be unable to pass statutes with stronger provisions or provisions tailored to individualized issues. Under the United States' federalist system, it is crucial that the federal government remain cautious in avoiding infringement upon state sovereignty. Lawmakers' primary concern surrounding the ADPPA was its preemption of state laws and the degree to which it infringed upon each state's right to create its own legislation. Due to this, drawing upon the approach of

[62] California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General, January 28, 2025. https://oag.ca.gov/privacy/ccpa.
[63] Id.
[64] *The People v. DoorDash (2024)*, CGC-24-612520 (Cal. 2024).
[65] American Data Privacy and Protection Act, H.R.8152, 117th Cong. (2021); American Privacy Rights Act, H.R.8818, 118th Cong. (2024).

the APRA in avoiding preemption is vital to creating a successful federal consumer data privacy statute.

The APRA has a preemption clause which states that no state may "adopt, maintain, enforce, or continue in effect any law, regulation, rule, or requirement covered by the provisions" of the APRA, however, a multitude of exceptions are included.[66] Due to the nature of the APRA's provisions and this clause's exceptions, the APRA allows stronger and more specific state laws to exist alongside it. This clause establishes the APRA as a baseline bill that states can build upon, which is crucial for a successful statute. However, a successful statute must be selective in the degree to which it preempts state statutes and must adequately avoid diluting the progress made by states. The Executive Director of the California Privacy Protection Agency (CPPA) noted that a federal statute must be a "floor" rather than a "ceiling" for privacy rights legislation.[67] The CPPA argues that since there are instances in which the APRA's preemption clause renders stronger state statutes void, California lawmakers will oppose bills of this nature.[68] To avoid this, a successful statute must act as a baseline that preserves states' progress when preemption occurs. This way, when preemption occurs, the statute will protect consumers in states without comprehensive data privacy statutes and remain on par with pre-existing protections in the states that do.

V. Conclusion

Congress should enact a comprehensive federal data privacy statute that sets a national baseline of consumer protections—drawing upon the California Consumer Privacy Act—while preserving states' ability to implement stronger safeguards, thereby avoiding the preemption pitfalls of past legislation and respecting the constitutional balance between federal authority and state sovereignty. However, a successful federal statute must omit the mistakes of the previously proposed comprehensive federal consumer privacy legislation and be strategic about preempting state laws. That is, the statute must be strong enough to preempt state laws in areas where necessary, while remaining broad enough for states to include their provisions. Modeling a comprehensive federal data privacy statute after the California Consumer Privacy Act is the best way to ensure success, as it is the oldest state data privacy statute and functioned as a model for the 19 states that followed suit in establishing their own. Its explicit outlining of consumer rights and firm enforcement methods serve as effective guidelines for application at the federal level.

As the world becomes increasingly digitized, consumer data will correspondingly become more exposed to sale and sharing by corporations. Capitalism fuels businesses' desire for consumer data since consumer data can be used to nonconsensually target consumers through unsolicited advertising and the promotion of products or ideas. Therefore, it is important to

[66] Benson, Peter J, et al., Summary of the American Privacy Rights Act, May 31, 2024. https://www.congress.gov/crs-product/LSB11161.
[67] Mahoney, Maureen. Legislative Update and Authorizing CPPA's Position on Pending Legislation, p. 3, May 10, 2024. https://cppa.ca.gov/meetings/materials/20240510_item3_profiling_legislation.pdf.
[68] Id. at p. 4.

protect consumers' right to privacy and regulate businesses' behavior. Each and every American is entitled to control what is done with their data, as it is essentially a form of digital property. Our federal system of law must adapt to suit modern-day Americans' needs and protect them from potential discrimination as a result of data misuse by corporations. While data protection may not be a concern at the forefront of every American's mind, its necessity will become more apparent as individuals' lives continue becoming more intertwined with the online world. Therefore, the federal government must be proactive in taking the necessary steps to grant each citizen the right to control their data, rather than leaving it unregulated and in the hands of corporations.