CALIFORNIA PRIVACY PROTECTION AGENCY
2101 ARENA BLVD.
SACRAMENTO, CA 95834
cppa.ca.gov

April 16, 2024

The Honorable Cathy McMorris Rodgers, Chair
House Energy & Commerce Committee
United States House of Representatives
Washington, DC 20515

The Honorable Gus Bilirakis, Chair
Innovation, Data, and Commerce Subcommittee
United States House of Representatives
Washington, DC 20515

Re: American Privacy Rights Act Discussion Draft

Dear Chairs McMorris Rodgers and Bilirakis,

In light of the Innovation, Data, and Commerce Subcommittee's hearing, "Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights," the California Privacy Protection Agency (Privacy Agency)[1] writes to urge the House Energy & Commerce Committee to consider comprehensive federal privacy legislation that truly protects Americans' privacy by setting a floor, not a ceiling on those rights. Instead, the American Data Privacy Rights Act discussion draft,[2] released just last week, includes language intended to eliminate nearly every provision in the California Consumer Privacy Act (CCPA),[3] the California Delete Act,[4] and other existing privacy laws—and seeks to prevent California and other states from further advancing protections.

In this era of rapid technological innovation, this approach is short-sighted. For years, California and other states have typically been the first to step in to address new threats to consumer privacy. In 2002, California became the first state to pass a data breach notification requirement, and in 2018, it became the first to adopt a comprehensive commercial privacy law, the California Consumer Privacy Act. That pace has only accelerated as technology has grown more advanced. In the past two years alone, California has adopted multiple pieces of legislation to strengthen privacy protections—including a first-in-the-nation global data broker deletion requirement[5] and new protections with respect to reproductive privacy.[6] These efforts are supported by the CCPA's unique "floor" on protections, ensuring that any amendments to the CCPA by the California legislature are in furtherance of the law's intent: to protect privacy.[7] This benefits not

[1] Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians' consumer privacy. The Agency implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.
[2] American Privacy Rights Act of 2024 Discussion Draft (APRA), https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf.
[3] Cal. Civ. Code § 1798.100 et seq.
[4] 2023 Cal. Stat. 709 (SB 362).
[5] *Id.*
[6] See, for example, 2022 Cal. Stat. 567 (AB 1194).
[7] Proposition 24 (2020), Sec. 25.

just Californians but all Americans since it provides a baseline of protections to which businesses must adhere.

If adopted, APRA could remove these and many other singular protections enjoyed by Californians. For example, the draft seeks to remove the California Privacy Protection Agency's (Privacy Agency) authority, overriding the will of California voters to create a new state data protection authority.[8] The CCPA provides the Privacy Agency with the power to audit and bring administrative actions against businesses under its jurisdiction, creating another law enforcement entity to protect consumer privacy.[9] California's unique audit authority, in particular, is modeled after European inspection authority. And though the APRA seeks to vest the Federal Trade Commission (FTC) with new responsibilities, it also prevents the FTC from bringing robust enforcement in certain scenarios by granting compliance safe harbors to businesses. Constraining the primary enforcement authority when Americans need greater privacy enforcement—and limiting existing privacy enforcers—disadvantages consumers.[10]

The APRA also seeks to undermine efforts to secure comprehensive protections with respect to emerging technologies like artificial intelligence, including automated decisionmaking technology (ADMT). Though not yet law, California is proposing draft regulations that already go farther than the APRA, including a right to opt-out of the use of personal information with respect to training ADMT.[11] The Privacy Agency's rulemaking authority also permits it to update regulations in response to changes over time, to keep pace with evolving technology. But as written, the APRA would lock the country into a standard that stymies California's rulemaking innovation.

In addition, APRA seeks to weaken protections with respect to data brokers. The California Delete Act, adopted last year, gives consumers the right to request that their personal information held by all registered data brokers be deleted, in a single step. If the consumer requests such deletion, businesses are also prevented from selling or sharing new personal information. And if a deletion request cannot be verified, the data broker must honor the request as an opt out of sale or sharing. Instead, APRA provides for a global data broker "Do Not Collect" request, which would still allow data brokers to retain and sell consumers' information—which is a significant security risk. Lastly, the APRA caps certain penalties for data brokers' noncompliance with registration and notice requirements to approximately $10,000 per year, which would weaken the law overall. The California Delete Act has no such cap.

APRA also lacks critical protections with respect to sexual orientation, union membership, and immigration status. Not including these categories in the definition of sensitive covered data leaves crucial gaps in protections. For example, APRA exempts inferences made from publicly available information as long as they do not reveal information about an individual that would constitute sensitive covered data and are not combined with covered data.[12] For example, if a business makes an inference that an individual is a member of the LGBT community based on factors such as social media posts and address, the business would not be obligated to disclose,

---

[8] Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians' consumer privacy. The Agency implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.
[9] Cal. Civ. Code § 1798.199.40
[10] APRA, Sec. 15
[11] California Privacy Protection Agency, Draft Risk Assessment and Automated Decisionmaking Technology Regulations (March 2024), https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf.
[12] APRA, Sec. 2(9)(iv).

correct, or delete this inference because it would not be "covered data." In contrast, the CCPA includes sexual orientation, union membership, and immigration status in the definition of sensitive personal information.[13] And the California Attorney General has clarified that inferences derived from publicly available information are covered by the CCPA.[14]

Traditionally, federal privacy legislation has set a baseline and allowed states to develop stronger protections. For example, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA), among others, include language that enables states to adopt stronger protection.[15] California has often done so. The Confidentiality of Medical Information Act and the California Financial Information Privacy Act are just two examples of California laws that build on the federal baseline.[16] This approach has not prevented California from becoming one of the largest economies in the world.[17]

The APRA would break with that tradition. In addition, it is not clear that the draft would create a single national standard, often cited as the justification for preempting state law. Requiring the FTC to bless compliance plans developed by different businesses could lead to a proliferation of procedures for exercising access, deletion, correction, and opt-out rights. This would shift the burden of compliance to consumers, especially seniors, parents of young children, and other underserved groups who do not have the resources to navigate hundreds if not thousands of different processes.

A federal privacy law with sweeping preemption language could freeze protections for the next thirty years. Strong federal protections do not have to come at the expense of the states. Indeed, if we view states as laboratories in our federal system, the APRA would slam the door closed when it comes to privacy and emerging technology.

We look forward to working with you to craft legislation that supports both a federal baseline and states' ability to innovate.

Sincerely,

Ashkan Soltani
Executive Director
California Privacy Protection Agency

cc: Members, House Energy & Commerce Committee

---

[13] Cal. Civ. Code § 1798.140(ae).
[14] Opinion No. 20-303 (Opinion), State of California Office of the Attorney General at 11 (Mar. 10, 2022), https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf.
[15] *See* 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 6807; 15 U.S.C. § 1681t.
[16] Cal. Civ. Code § 56.10 et seq.; Cal. Fin. Code § 4051(b).
[17] Office of Governor Gavin Newsom, *ICYMI: California Poised to Become World's 4th Biggest* Economy (Oct. 24, 2022), https://www.gov.ca.gov/2022/10/24/icymi-california-poised-to-become-worlds-4th-biggest-economy/.