

CALIFORNIA PRIVACY PROTECTION AGENCY

2101 Arena Blvd
Sacramento, CA 95834
www.cppa.ca.gov

**M e m o r a n d u m**

Date: July 26, 2022

To: California Privacy Protection Agency Board
(Meeting of July 28, 2022)

From: Maureen Mahoney, Deputy Director of Policy and Legislation

Subject: Analysis and Recommended Agency Position on Federal Legislation, H.R. 8152: The American Data Privacy and Protection Act (Version: July 22, 2022)

Description: H.R. 8152, The American Data Privacy Protection Act (ADPPA) seeks to preempt nearly all provisions of the California Consumer Privacy Act of 2018 (CCPA), as amended by Proposition 24, the California Privacy Rights Act of 2020 (CPRA), and additional privacy legislation such as California's data broker registry law. California's private right of action for a negligent data breach, in Cal. Civ. Code Sec. 1798.150, is explicitly carved out, and provisions in the CCPA that govern protections of employees and students, for example, would continue to be valid. However, most protections Californians currently enjoy under the CCPA would likely be preempted, including, notably, the CCPA's "floor" for privacy protections, California's ability to strengthen the law in the future, and the Agency's ability to protect Californians' privacy rights under the California law.

Brief Summary of Bill and Status:

Brief Summary—ADPPA is federal privacy legislation that provides the right to access, delete, and correct covered data, with additional protections for sensitive covered data. It seeks to broadly preempt state privacy laws like the CCPA, the Colorado Privacy Act, the Connecticut Data Privacy Act, Maine's broadband privacy law, and data broker registry laws in California and Vermont, but provides specific carveouts for some sectoral privacy laws, such as those relating to employee and student privacy, some specific laws such as Illinois's Biometric Information Privacy Act (BIPA), and portions of certain laws, such as the negligent data breach private right of action in the CCPA. As drafted, it would likely limit the ability of the Agency to fulfill its mandate and prevent the Agency and the California legislature from strengthening privacy protections in the future.

Status—ADPPA was advanced by the House Committee on Energy & Commerce on July 20, 2022. Staff from the Agency have engaged with the authors and the California delegation to provide technical information about how the ADPPA would interact with privacy protections guaranteed to Californians under the CCPA (and the California Constitution). The Governor, Speaker of the Assembly, and the California Attorney General have all submitted letters critical of the broad preemption language in the bill. Representative Eshoo proposed an amendment during the House Committee on Energy & Commerce's markup of the bill on July 20, 2022, that would have allowed states to adopt stronger privacy protections. Though that amendment was not adopted, all members of the California delegation

on the Committee voted in favor of it. Representatives Eshoo and Barragan voted against the bill in Committee.

Analysis: ADPPA would extend certain privacy protections to states where they do not currently exist. However, due to its broad preemption language, ADPPA would likely have significant effects on California law. These include:

- Removing the unique “floor” for privacy protections created by the CPRA. The CPRA amendments to the CCPA state that “The provisions of this Act may be amended after its approval by the voters by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor, provided that such amendments are consistent with and further the purpose and intent of this Act...” This means that, currently, California enjoys a “floor” of privacy protections. However, ADPPA seeks to preempt this floor along with other provisions of the CCPA. This means that Congress could weaken Californians’ privacy protections in the future by weakening the ADPPA. This would be a substantial change from current California law.
- Creating a “ceiling” on privacy protections for Californians that could be raised only by Congress. The preemption provisions in ADPPA, in addition to removing California’s “floor” on privacy protections, would also prevent California from strengthening the law in the future. This would immediately affect several privacy bills advancing through the California legislature in its current session, including bills to strengthen protections for kids’ data (for those under 18), to protect smart speaker data, and to protect video collected by in-car cameras, that likely would be preempted by ADPPA. And it would prevent future fixes by the California legislature, by California regulation, or by citizen ballot initiative, intended to respond to future threats to Californians’ privacy. Other states would also not be able to respond on behalf of their citizens.
- Substantially affecting the Agency’s ability to fulfill its responsibilities as mandated by the CPRA. In passing the CPRA, Californians created the Agency and vested it with the responsibility and authority to implement and enforce the CCPA. This includes issuing regulations, auditing businesses’ compliance, and providing administrative enforcement of the CCPA on behalf of Californians. Preempting most of the substantive provisions of the law that created the Agency, as ADPPA seeks to do, would nearly eliminate the Agency’s ability to carry out its mandate of protecting the privacy of California residents under California law.

ADPPA currently purports to provide the Agency with the ability to enforce the new federal law. However, the language in the bill still raises significant uncertainties for the Agency were it to seek to enforce the federal bill, as the California legislature may need to take separate action to give the Agency the ability to enforce the federal law. Further, the bill as currently drafted arguably does not permit California to recover the monetary penalties associated with its enforcement of the federal law, whereas the CCPA currently allows recovery of significant penalties for the violations of the CCPA.

- Replacing many provisions of the CCPA. In some cases, ADPPA provisions would provide substantially less protection to Californians than they currently enjoy under the CCPA, as amended by the CPRA. For example:

- Removing the current opt out of automated decision-making. CPRA directs the Agency to develop regulations providing access and opt-out (objection) rights with respect to automated decision-making, and requiring meaningful information about the logic of decision-making pursuant to access; protections that are not included in the federal bill. These protections cover more entities and types of automated processing that ADPPA’s impact assessments for risky automated decisions, and they put consumers in control of whether they will be subject to such decision-making. These are crucial components of any privacy and civil rights law.
- Replacing the definition of “personal information” currently covered by the CCPA with a definition of “covered data” that does not include some important types of information protected by the CCPA. The CCPA’s definition of personal information specifically includes unique identifiers and inferences. In addition, the California Attorney General has recently issued an opinion to clarify that inferences from publicly available documents are covered by the CCPA. In contrast, ADPPA’s recently-adjusted definition of covered data “*may* include derived data and unique identifiers.” (emphasis added). ADPPA also exempts “inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.” Finally, recent changes to the ADPPA’s definition of deidentified information create additional loopholes.
- Removing certain protections with respect to non-retaliation for exercising privacy rights. ADPPA would remove the CCPA’s requirement that financial incentives practices with respect to exercising privacy rights not be “unjust, unreasonable, coercive, or usurious in nature.” This is an important backstop to prevent exploitative practices.
- Adding a requirement to authenticate global opt-out requests. California requires businesses to honor browser privacy signals as an opt out of sale, and authentication of such requests is not required. This is to prevent hundreds of businesses from contacting the individual to confirm the opt out one-by-one and to prevent targeted advertising loopholes. ADPPA’s global opt out has recently been amended to include an authentication requirement for global opt-out requests.
- Removing privacy and security risk management obligations for some businesses whose data processing creates a risk to consumers. CCPA creates obligations for cybersecurity audits and data protection impact assessments (DPIAs) on “businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security,” not just entities that are “large data holders,” as in ADPPA. This is designed to balance the impact to businesses while addressing small data brokers that might process sensitive information.
- Replacing important enforcement provisions. California law provides significant power to the Agency to audit businesses under its jurisdiction, authority that the Federal Trade Commission (FTC) does not have. In addition, ADPPA provides businesses compliance safe harbors that do not exist in the CCPA.

Recommendation: Oppose

Attachments: Letter from Governor Gavin Newsom to Chairman Pallone re: ADPPA; Letter from Attorney General Rob Bonta and Nine Attorneys General to Congressional Leaders re: ADPPA, Letter from California Assembly Speaker Anthony Rendon to United States House of Representatives Speaker Nancy Pelosi re: Federal Preemption of California's Landmark Privacy Law.

Staff Contact:

Maureen Mahoney, Deputy Director, Policy and Legislation, maureen.mahoney@coppa.ca.gov