How the American Data Privacy and Protection Act (ADPPA) Compromises Californians' Privacy Protections
July 1, 2022

On June 23, 2022, the House Energy & Commerce Consumer Protection Subcommittee advanced H.R. 8152, The American Data Privacy Protection Act (ADPPA). While the bill would extend privacy protections to states where they do not currently exist, as introduced, this measure seeks to preempt nearly all provisions of the California Consumer Privacy Act (CCPA), as amended by Proposition 24, the California Privacy Rights Act of 2020 (CPRA), except for California's private right of action for a negligent data breach, in Cal. Civ. Code Sec. 1798.150. This could remove protections from Californians, likely including nearly all of the authority for the California Privacy Protection Agency (CPPA), the independent agency that implements regulations and will provide administrative enforcement of the law; California's unique privacy floor that prevents protections from being weakened in the future; could preclude the California legislature (and the public through the ballot initiative) from adding new, stronger protections; and compromise additional existing protections. Below, we explain in more detail how ADPPA's preemption approach would hurt Californians.

ADPPA seeks to remove the unique "floor" on CA privacy protections. Because the CPRA was passed by a ballot initiative, and the initiative holds that amendments to the act must be in furtherance of the privacy intent of the measure, California enjoys a floor of privacy protections that cannot be weakened (CPRA Sec. 25). This provision allows the California State Legislature, with the Governor's approval, to amend the law to strengthen privacy protections, but does not allow the measure to be weakened by future amendments that are incompatible with the purpose and intent of the act: to strengthen consumer privacy. However, ADPPA proposes to eliminate those protections.

ADPPA proposes to eliminate nearly all of the authority of the California Privacy Protection Agency (CPPA), with its singular expertise and enforcement capabilities. ADPPA seeks to remove nearly all of the CPPA's authority and, as written, likely would not permit it to enforce the federal measure. The ballot initiative created and funded an expert agency, the California Privacy Protection Agency, with a primary focus on privacy and data protection. The initiative enlists the Agency to issue implementing regulations and, along with the Attorney General, to enforce these rights. Since the CPPA was created by ballot initiative, preempting the law that created it could eliminate the Agency's authority to issue regulations and enforce the state law. Further, with respect to CPPA enforcement of the federal measure, while ADPPA states that a State Privacy Authority can take *civil* action to enforce the ADPPA, the definition of state privacy authority does not adequately identify the CPPA, nor can the Agency take civil action, since it has *administrative* enforcement authority only. Even if these issues were fixed, because the CPPA only has authority with respect to the state law, the California legislature likely would need to take separate action to give the Agency the ability to enforce the federal law. It's particularly inappropriate to undermine an existing agency that was created through ballot initiative—directly by California voters.

ADPPA could reduce resources to protect Californians' privacy. California law also provides significant power to the Agency to audit businesses under its jurisdiction (Cal. Civ. Code Sec. 1798.185(a)(18)). This allows the Agency to audit business's compliance without bringing an enforcement action—ensuring that the law is upheld without costly litigation. The Federal Trade Commission does not have that authority under the ADPPA. In addition, the Agency is guaranteed $10 million per year by the CPRA, and the legislature may also allocate additional funds to the CPPA as well. Privacy-specific staffing is projected to match what currently exists at the Federal Trade Commission. Removing these resources, especially when the ADPPA asks the FTC to take on several significant new rulemakings and to greatly expand its privacy enforcement work, without providing additional funds, would decrease protections for Californians.

ADPPA has weaker protections with respect to non-retaliation for exercising privacy. rights. Under both the CCPA and the ADPPA, businesses can charge consumers for exercising their privacy rights, but only CCPA has a requirement that financial incentives practices not be "unjust, unreasonable, coercive, or usurious in nature." (Cal. Civ. Code Sec. 1798.140(b)(4)). This is an important backstop to help avoid some of the worst practices, in which a consumer could be forced to choose between their fundamental privacy rights and being able to afford essential services like internet service. This is particularly important for Californians, who have an explicit right to privacy under the California Constitution. (Cal. Const. Art. 1 Sec. 1) However, such protections are not included in the federal bill.

ADPPA does not contemplate an opt-out of automated decision-making. ADPPA requires annual impact assessments for algorithms to help rein in harmful practices, but unlike California there is no language providing access and opt out rights with respect to automated decision-making, including profiling and requiring meaningful information about the logic of decision-making pursuant to access requests. CPRA directs the CPPA to develop regulations to that effect (Cal. Civ. Code Sec. 1798.185(a)(16)). This could be particularly important for consumers seeking to opt out of automated decision-making in housing or employment decisions.

ADPPA would delay a global opt-out requirement that Californians currently have. CCPA regulations currently require businesses to honor browser privacy signals as a global opt out of sale—so that consumers can exercise their opt-out preferences for all companies in a single step —and the Attorney General is currently enforcing that requirement. Prop. 24 adds the browser privacy signal requirement to the statute and expands it to cover data sharing as well. CPPA has proposed regulations that clarify that the requirement is mandatory (Sec. 7025). While the ADPPA would require businesses to honor a global opt out mechanism, the FTC has 18 months to clarify the outlines of that requirement, potentially preventing Californians from enjoying those protections in that interim.

ADPPA has a weaker definition of covered information. ADPPA's recently adjusted definition of covered data "means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and *may* include derived data and unique identifiers." (emphasis added). CPRA's definition of personal information "means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household[,]" including, specifically, unique identifiers (Cal. Civ. Code Sec. 1798.140(v)(1)(A)). In addition, The California Attorney General has recently issued an opinion to clarify that inferences (derived data) are covered by the CCPA's right to know. However, this is less clear in ADPPA. These differences could exempt key information that could be used to target advertising, including, potentially, with respect to reproductive privacy.

ADPPA seeks to preclude California from strengthening its protections. Beginning at least in 2002, when California adopted the first data breach notification law in the United States; in 2018, when it adopted special security protections for connected devices and the first comprehensive commercial privacy law in the United States, the CCPA; and in 2020, when it created the first European-style data protection authority, the CPPA, California has always been at the forefront of protecting consumer data. By seeking to broadly preempt privacy measures except for a few sectoral areas and a few specific statues in other states, ADPPA could largely prevent the California legislature—and the public through the ballot initiative process—from strengthening privacy and data security law further. This year alone there are several privacy bills advancing through the California legislature, including to strengthen kids' data (for those under 18), smart speaker data, and video collected by in-car cameras. These are just a few examples of bills that may well be adopted this year—to say nothing of bills that may be adopted in subsequent years.

Further, the CPPA has broad authority under the CPRA to issue regulations on areas delineated in the statue and to "adopt additional regulations as necessary to further the purposes of this title." On May 26, 2022, the Agency released draft proposed regulations to implement several provisions of the CPRA. The initial package was approved by the California Privacy Protection Agency Board on June 8, and shortly, the CPPA will begin the formal rulemaking process. Rulemaking could provide an opportunity to expand protections as needed in response to changing technologies, typically more quickly than the FTC. Thus, adopting ADPPA as written could halt timely privacy improvements for Californians.

Carving out California is consistent with interoperability. CPRA was intended to harmonize protections with the European Union's General Data Protection Regulation (GDPR), and the CPPA was modeled after European data protection authorities. In addition, in its basic structure, the ADPPA reflects California law. And part of the CPPA mandate is to "Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections." (Cal. Civ. Code Sec. 1798.199.40(i)). Carving California out of the federal law would support continued timely updating of privacy and security protections in a way that that is consistent with interoperability.

While extending privacy protections nationwide is important, under this bill, it would come at the expense of Californians' rights. For more information or to discuss further, please contact Maureen Mahoney, Deputy Director of Policy and Legislation, California Privacy Protection Agency (maureen.mahoney@cppa.ca.gov)