State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

May 8, 2024

Dear Congressional Leaders:

We, the undersigned Attorneys General, write to express our perspective on Congress's recent effort to advance national consumer privacy legislation with the introduction of the American Privacy Rights Act (APRA). As the chief consumer protection officials in our respective states, we hope that Congress's work can be informed by our efforts to enact and enforce data security and privacy laws while industry rapidly innovates. We encourage Congress to adopt legislation that sets a federal floor, not a ceiling, for critical privacy rights and respects the important work already undertaken by states to provide strong privacy protections for our residents. A federal legal framework for privacy protections must allow flexibility to keep pace with technology; this is best accomplished by federal legislation that respects—and does not preempt—more rigorous and protective state laws.

We are heartened by many provisions in the APRA: for example, data minimization by default, strong consent requirements, and critical protections for minors under 17 years of age. And while we welcome new federal protections, any national privacy bill cannot foreclose the states from continuing to legislatively innovate to protect our consumers. Since California passed the first comprehensive privacy law in 2018, other states have followed suit: Colorado, Connecticut, Maryland, Virginia, Utah, Iowa, Indiana, Tennessee, Oregon, Montana, Texas, Delaware, Florida, New Jersey, New Hampshire, and Kentucky all have laws that vest consumers with new rights over their personal information. Many Americans are (or will soon be)[1] enjoying their existing privacy rights and businesses have developed mechanisms to respond to consumers exercising their rights, including online user-enabled global opt-out mechanisms, like the Global Privacy Control.[2] As the APRA is currently drafted, Americans will have to wait an additional two years to exercise their privacy rights via the Global Privacy Control until rulemaking is completed. Even as Congress debates the proposed legislation, we urge you to ensure such legislation does not undermine protections that states have already established.

[1] The consumer privacy laws recently enacted in Florida, Oregon, and Texas, which collectively cover approximately 16.4% of the U.S. population, take effect on July 1, 2024.

[2] The Global Privacy Control is one example of how the setting of new minimum data privacy standards by states has spurred new technologies and technological advancement and not impeded business or curtailed innovation.

In addition to comprehensive consumer data privacy laws, states have passed innovative consumer protection laws requiring reasonable data security safeguards[3], establishing special protections for data that could be used to commit identity theft[4], or mandating consent before collecting biometric data or processing health-related data. States have played a critical role in nimbly adapting to real-world circumstances and setting new minimum data privacy standards that have not impeded business or curtailed technology. Congress should seek to preserve, not jeopardize, these protections.

Congress should adopt a federal baseline, and continue to allow states to provide additional protections for consumers residing in their jurisdictions. This approach has been successful in other consumer privacy contexts, including laws relating to children's privacy, financial privacy, and health privacy.[5] For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides a national floor for privacy protections for individuals' individually identifiable health information, giving State Attorneys General concurrent enforcement authority and only preempting State laws that are "contrary." (45 C.F.R. § 160.203). Accordingly, California provides additional protections for patient privacy in its Confidentiality of Medical Information Act (Cal. Civ. Code, § 56, et. seq.), which led to its enforcement action against Glow, Inc., a technology company that operates mobile applications marketed as fertility and women's health trackers and had basic security failures that put its users' data at risk.

Similarly, the Children's Online Privacy Protection Act (COPPA), which has not been amended since its passage, preempts only state laws that are "inconsistent" with the statute's treatment of regulated activities. (15 U.S.C. §§ 6502(d)). As a result, states including California, Oregon and Connecticut have enacted laws regulating the data collection and use practices of Education Technology providers that might also be "operators" under COPPA.[6] State laws can and should bolster privacy protections where there are violations of federal law. Our state residents benefit directly from more protective state laws complemented by rigorous enforcement.

Any federal privacy framework must leave room for states to legislate responsively to changes in technology and data collection practices. This is because states are better equipped to quickly adjust to the challenges presented by technological innovation that may elude federal oversight. For example, when the states began enacting data breach notification laws in 2003, biometric data was not widely used by consumers as a tool for identity authentication. Now, biometric information is part of our everyday life. Accordingly, the states acted to amend our laws to add required notification in the event of a breach of biometric data.[7] Likewise, the

---

[3] *See*, e.g., Conn. Gen. Stat. § 42-471 (requiring the safeguarding of personal information).

[4] See, e.g., Conn. Gen. Stat. § 36a-701b (requiring that companies offer impacted Connecticut residents appropriate protection services in the wake of breaches involving sensitive personal information).

[5] See 15 U.S.C. § 6502(d); 15 U.S.C. § 6807; 45 C.F.R. Part 160, Subpart B.

[6] Cal. Bus. & Prof. § 22584 (2015); Or. Rev. Stat. § 336.184 (2015); Conn. Gen, Stat. §10-234aa-dd (2016); Md. Code, Educ. § 4-131 (2015).

[7] *See, e.g.*, Cal. Civ. Code § 1798.82; Colo. Rev. Stat. § 6-1-716; Conn. Gen. Stat. § 36a-701b.

proliferation of genetic and DNA testing in and out of the health care context has led states to update breach statutes to cover genetic information and/or enact genetic privacy laws.[8] Similarly, states have responded to evolving technology by legislating new requirements that protect consumers; for example, Connecticut recently enacted and California recently proposed legislation to prohibit social media platforms from providing addictive feeds to minors under the age of 18.[9] States should be assured continued flexibility to adapt their state laws to respond to changes in technology and information privacy practices, and align our enforcement efforts with those areas most affecting our respective residents.[10]

Finally, the APRA includes language that poses an additional concern for some states. While we appreciate that the legislation articulates a specific role for enforcement by state Attorneys General, the bills as drafted appear to substantially preempt many states' ability to investigate. Section 20 preserves state consumer laws and causes of action, but the text in subdivision (c) provides that "a violation of this Act or a regulation promulgated under this Act may not be pleaded as an element of any violation of such law." In many states, the Attorney General's office uses civil investigative demands under its consumer protection authority to demand documents or information from entities when we believe there could have been a violation of a law.[11] Ordinarily, a violation of a federal law or standard could also be a violation of state consumer protection law. But Section 20 would act as a bar to investigate violations of the federal law, because it prohibits them from forming the basis for state consumer protection claims. This language unnecessarily interferes with robust enforcement capabilities.

We welcome a federal partner with the tools and resources for vigorous enforcement of new consumer rights. But it is critical that Congress set a federal privacy-protection floor, rather than a ceiling, to continue to allow the states to innovate to regulate data privacy and protect our residents. As you and your colleagues debate provisions of the proposed bill, we hope you take into consideration the comments we have provided here.

Sincerely,

ROB BONTA
California Attorney General

WILLIAM TONG
Connecticut Attorney General

[8] Or. Rev. Stat. § 192.531 (2023); Md. Code, Com. § 14-3501 (2023); Md. Code, Com. § 14-4401 (2023).

[9] Connecticut Senate Bill 2 (2023) (eff. October 1, 2024); Sen. 976 (Cal. 2023-2024).

[10] In another example, Massachusetts recently issued an advisory on the Application of the Commonwealth's Consumer Protection, Civil Rights, and Data Privacy Laws to Artificial Intelligence, a very recent and rapidly expanding area of technology. See: Mass. Att'y Gen., AG Campbell Issues Advisory Providing Guidance On How State Consumer Protection And Other Laws Apply To Artificial Intelligence (2024), https://www.mass.gov/news/ag-campbell-issues-advisory-providing-guidance-on-how-state-consumer-protection-and-other-laws-apply-to-artificial-intelligence

[11] *See, e.g.*, Mass. Gen. L. c 93A, § 6; Nev. Rev. Stat. § 598.0963(4).

KATHLEEN JENNINGS
Delaware Attorney General

BRIAN L. SCHWALB
District of Columbia Attorney General

MANA MORIARTY
Executive Director
State of Hawaii Office of Consumer Protection[12]

KWAME RAOUL
Illinois Attorney General

AARON M. FREY
Maine Attorney General

ANTHONY G. BROWN
Maryland Attorney General

ANDREA CAMPBELL
Massachusetts Attorney General

KEITH ELLISON
Minnesota Attorney General

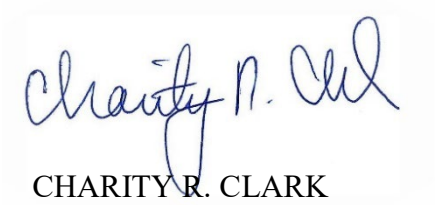
AARON D. FORD
Nevada Attorney General

LETITIA JAMES
New York Attorney General

[12] Hawaii is represented on this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity purposes, the entire group will be referred to as the "Attorneys General" or individually as "Attorney General" and the designations, as they pertain to Hawaii, refer to the Executive Director of the State of Hawaii's Office of Consumer Protection.

ELLEN F. ROSENBLUM
Oregon Attorney General

MICHELLE A. HENRY
Pennsylvania Attorney General



CHARITY R. CLARK
Vermont Attorney General