



State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

July 19, 2022

Dear Congressional Leaders:

We, the undersigned Attorneys General, write to express our perspective on the recent efforts in Congress to advance national consumer privacy legislation, such as through the American Data Privacy and Protection Act (ADPPA) and the Consumer Online Privacy Rights Act (COPRA). 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.

Since California passed the first comprehensive privacy law in 2018, other states have followed suit: Colorado, Connecticut, Virginia, Utah, and Nevada all have laws that vest consumers with new rights over their personal information. Other states have passed innovative consumer protection laws requiring reasonable data security safeguards, establishing special protections for data that could be used to commit identity theft, or mandating consent before collecting biometric 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. As Congress debates the proposed legislation, we urge you to ensure such legislation does not undermine protections that states have already established.

Congress should adopt a federal baseline, and continue to allow states to make decisions about 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 and health privacy. 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 (CMIA). (Cal. Civ. Code, § 56, *et. seq.*) California relied on the CMIA to file an action against Glow, Inc., a technology company that operates mobile applications marketed as

fertility and women’s health trackers. As a health app, Glow was *not* subject to HIPAA; but Glow was required to, and failed to, comply with the CMIA. Glow’s app had basic security failures that put its users’ data at risk, which in addition to the CMIA, triggered violations of California’s data security law, the California Online Privacy Protection Act, and our Unfair Competition Law.

State laws can also bolster privacy protections where there *are* violations of federal law. For example, Connecticut was the first state to exercise its HIPAA enforcement powers against Health Net of Connecticut, Inc., after Health Net failed to timely report the theft of a disk containing more than half a million Connecticut residents’ protected health information. Connecticut alleged HIPAA violations as well as state law claims for violation of its breach notification law and the Connecticut Unfair Trade Practices Act. State residents benefitted directly from the resulting settlement as it provided various protections for impacted consumers, including credit monitoring, identity theft insurance, and reimbursement for security freezes. Today, Connecticut’s breach notification law requires businesses to provide impacted Connecticut residents with two years of free identity theft prevention and, if applicable, mitigation services for breaches involving Social Security or taxpayer identification numbers—strengthening protections for victims of HIPAA data breaches.¹ As another example, in the context of data security, Massachusetts filed suit against Equifax after its massive 2017 data breach for violations of its state data security regulations, 201 Code Mass. Regs. 17.00 *et seq.*

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.² Similarly, states have responded to evolving technology by legislating new requirements that protect consumers; for example, California passed a law in 2018 requiring reasonable data security for internet-connected devices (“Internet of Things” or IOT), after an uptick in malware attacks that exploit poorly secured household connected devices.³ 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.

¹ Conn. Gen. Stat. § 36a-701b. Connecticut’s Safeguards Law, Conn Gen. Stat. § 42-471, also establishes a guaranty fund through which consumers may be reimbursed for losses stemming from a business’s failure to safeguard their personal information.

² See, e.g., Cal. Civ. Code § 1798.82; Colo. Rev. Stat. § 6-1-716; Conn. Gen. Stat. § 36a-701b.

³ See also Maine’s “Act to Protect the Privacy of Online Customer Information,” 35-A M.R.S. § 9301.

Moreover, one portion of the preemption language within both the ADPPA and COPRA poses an additional concern for some states. While we appreciate that the drafts articulate a specific role for enforcement by state Attorneys General, the bills as drafted appear to substantially preempt many states' ability to investigate. Section 404 preserves state consumer laws and causes of action, but the text in subdivision (c) provides that "a violation of this Act shall not be pleaded as an element of any such cause of action." 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.⁴ Ordinarily, a violation of a federal law or standard could also be a violation of state consumer protection law. But Section 404 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



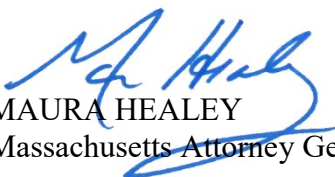
WILLIAM TONG
Connecticut Attorney General



KWAME RAOUL
Illinois Attorney General



AARON M. FREY
Maine Attorney General



MAURA HEALEY
Massachusetts Attorney General



AARON D. FORD
Nevada Attorney General

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

Congressional Leaders

July 19, 2022

Page 4



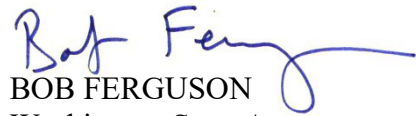
MATTHEW J. PLATKIN
Acting New Jersey Attorney
General



HECTOR BALDERAS
New Mexico Attorney General



LETITIA A. JAMES
New York Attorney General



BOB FERGUSON
Washington State Attorney
General