State of California
Office of the Attorney General
Xavier Becerra
Attorney General

Testimony of Xavier Becerra, California Attorney General

Hearing of the U.S. Senate Committee on Commerce, Science, and Transportation

"Revisiting the Need for Data Privacy Legislation"

September 23, 2020

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029

State of California
Office of the Attorney General
Xavier Becerra
Attorney General

Thank you, Chairman Wicker, Ranking Member Cantwell and Members of the Committee for the opportunity to address you here today. It is my privilege to testify before the Committee on Commerce, Science and Transportation on the subject of data privacy.

I want to start by thanking the committee for your ongoing efforts to advance legislation to extend much-needed privacy rights to consumers across the country. I hope that your work will be informed by our undertaking in California and the initiatives unfolding in so many of our states.

In the data privacy space, the optimal federal legal framework recognizes that privacy protections must keep pace with innovation, the hallmark of our data-driven economy. State law is the backbone of consumer privacy in the United States. Federal law serves as the glue that ties our communities together. To keep pace, we must all work from the same baseline playbook, but be nimble enough to adapt to real-world circumstances on the field where we meet them. I urge this committee to proceed in your work in a manner that respects—and does not preempt—more rigorous state laws, including those we have in California. Today I am here to share California's experience with a robust legal framework for consumer privacy.

California's Legal Framework for Consumer Privacy

In California, the right to privacy is enshrined in our state Constitution. California has been at the forefront of state privacy legislation, and our legal framework continues to evolve to keep pace with technology and changing norms. For example, in 2003, California became the first state to enact a data breach notification law. Now, 17 years later, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach laws inspired by or based on California's groundbreaking statute. We continue to refine and build on our laws to protect our residents. As recently as last year, California amended its data security laws to include protections for biometric information, as identity verification moves from things we have (physical objects like credit cards) or details we know (passwords and numbers), to what we are (biometrics). Protecting these data points is core to our liberties.

Having state privacy laws is essential to protect consumers and hold accountable those who commerce in data. Without our state laws, we would not have obtained a judgment against Equifax for breaching the confidentiality of over 15 million Californians' and

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029

148.8 million Americans' Social Security numbers. California's privacy framework provided critical leverage to negotiate the largest civil penalty for a data breach in history and robust injunctive terms that begin to move the company away from dependence on these numbers for identity verification.

California's data security and data breach reporting laws facilitated a groundbreaking settlement with Uber. The company initially attempted to cover up a breach of driver's personal information, including names and driver's license numbers. California used its robust laws and incorporated principles that the FTC has advocated for years to achieve this settlement. In addition to securing $148 million in penalties, our settlement requires the company to incorporate "privacy by design" into its products, putting privacy considerations at the forefront of design processes rather than as an afterthought for compliance review. The Uber settlement is an excellent example of how state and federal agencies can learn and build from one another to better protect our residents.

Privacy laws that can meet the moment not only protect consumers but lead to meaningful enforcement. That enforcement is critical to secure real-time accountability from violators which, in turn, increases deterrence. Last week, my office filed and settled an action against Glow, Inc., a technology company that operates mobile applications marketed as fertility and women's health trackers. It was reported that the "Glow app" had serious privacy and basic security flaws. In our complaint, we alleged that Glow was required to, yet failed to comply with, our state medical privacy law, the Confidentiality of Medical Information Act, which went beyond the floor established by the federal privacy law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), in addition to our data security law, the California Online Privacy Protection Act, and our Unfair Competition Law. In a settlement not driven by distressing headlines splashed on the news, the company agreed to reform its business practices to comply with these critical state privacy protections.

California Consumer Privacy Act

In 2018, California boldly took the first step to empower consumers with new privacy tools and new privacy rights, with the passage of the California Consumer Privacy Act (CCPA). Once again, our groundbreaking law has generated interest from international, national and state regulators. This new law is a game changer.

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029

Californians now enjoy the right to know, the right to delete, and the right to opt out of sale. They can find out what categories of personal information a business collects about them, as well as the specific pieces of personal information obtained. Californians can request that businesses delete information collected from them, subject to specific exceptions. Businesses must provide notice to consumers at or before the time that the consumer's data is collected, which is essential to how consumers understand what the business's privacy practices are and promotes greater transparency. And for the first time in a legal regime, the CCPA vests consumers with the right to tell a business that sells information: don't. This right is particularly robust when it involves personal information of minors, requiring that those under the age of 16 provide affirmative, opt-in consent, and for children under 13, consent must be provided by the child's parent or guardian. Finally, Californians have the right not to be treated differently if they exercise any of their CCPA rights, with some exceptions.

My office worked hard for the last two years to promulgate regulations that operationalize the CCPA for businesses and guide consumers in exercising their rights. Our regulations provide guidance on how businesses should create procedures to handle and respond to consumer requests to know what information a business has collected about them, to delete personal information, and to opt out of sale of that information. Our rules interpret how businesses verify the identity of consumers who make requests to know and requests to delete. They provide flexibility for businesses to adapt their practices, and they balance the risk of harm to consumers in the mishandling of their data. Finally, our regulations require that businesses disclose any financial incentives offered in exchange for a consumer's personal information and explain how these incentives are reasonably related to the value of the consumer's data. For the first time, with the CCPA, the curtain will be pulled back and we will be able to see how businesses value consumer data.

I know that businesses are working hard to adapt their privacy practices, as they have with any legal regime that establishes new obligations. The CCPA has paved the way for companies to innovate and extend to consumers outside of California the benefit of that innovation for privacy. Microsoft—whose Chief Privacy Officer is testifying here today—has indicated that it will extend CCPA protections and rights to all Americans, not just Californians. Other large companies will follow Microsoft's lead because privacy is good for business and competition. The CCPA will continue to spur innovation, as we see vendors offering new compliance products and services and start-ups launching to help consumers effectuate their privacy requests.

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029

Starting July 1, 2020, we began issuing notices to cure to companies with non-compliant privacy policies or missing "Do Not Sell My Personal Information" links. We are verifying that service provider contracts specify limitations on the use personal information. We continue to conduct investigative sweeps and review consumer complaints. Overwhelmingly, we have seen substantial compliance.

Recommendations for Further Action

Like any law, the CCPA is not perfect, but it is an excellent first step. Consumers deserve more privacy and easier tools. For example, in the regulations implementing the CCPA, the California Department of Justice tried to address the frustration of consumers who must proceed website-by-website, browser-by-browser in order to opt out of the sale of their personal information. One provision of our regulations intended to facilitate the submission of a request to opt-out of sale by requiring businesses to comply when a consumer has enabled a global privacy control at the device or browser level, which should be less time-consuming and burdensome. I urge the technology community to develop consumer-friendly controls to make exercise of the right to opt out of the sale of information meaningful and frictionless. Making technology work for consumers is just as important as the benefits businesses receive in innovating.

There are also ways in which CCPA could go further and require refinement of its compliance measures. For example, the CCPA currently only requires disclosure of "categories of sources" from which personal information is collected and "categories of third parties" to whom personal information is sold. More specific disclosures, including the names of businesses that were the source or recipient of the information, should be required so that consumers can know the extent to which their information has been shared, bartered, and sold. If I receive junk mail from a company, I should be able to find out how it got my address and to whom it shared the information so I can stop the downstream purchase of my personal data. For now, businesses are not legally required to share that granularity of information. Consumers should also have the ability to correct the personal information collected about them, so as to prevent the spreading of misinformation.

On a broader level, if businesses want to use consumers' data, they should have a duty to protect and secure it, and wherever feasible, minimize data collection. Businesses should no longer approach consumer data with the mindset, "collect now, monetize later." There should be a duty imposed to use a consumer's personal information in accordance with

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029

the purposes for which the consumer allowed its collection, and in the consumer's interest, especially with the collection and storage of sensitive information, like precise geolocation. Although CCPA requires transparent notice at collection, moving beyond a notice-and-consent framework to contemplate use limitations would make our privacy rights more robust and balanced.

We need clear lines on what is illegal data use from the context of civil rights protections. Indirect inferences based on personal information should not be used against us in healthcare decisions, insurance coverage or employment determinations. We need greater transparency on how algorithms impact people's fundamental rights of healthcare, housing and employment, and how they may be perpetuating systemic racism and bias. Predatory online practices, such as increased cross-site tracking after a user browses healthcare websites, must be addressed.

Finally, new laws should include a private right of action to complement and fortify the work of state enforcers. While my office is working hard to protect consumer privacy rights in California, and our sister states do the same in their jurisdictions, we cannot do this work alone. While we endeavor to hold companies accountable for violations of privacy laws, trying to defend the privacy rights of 40 million people in California alone is a massive undertaking. Violators know this. They know our scope and reach are limited to remedying larger and more consequential breaches of privacy. Consumers need the authority to pursue remedies themselves for violations of their rights. Private rights of action provide a critical adjunct to government enforcement, and enable consumers to assert their rights and seek appropriate remedies. Consumer privacy must be real, it deserves its day in court.

Conclusion

Now, more than ever, consumers are demanding tools to protect their privacy. We all know that consumer personal information is packaged and sold to the highest bidder. Californians and all Americans need robust tools that allow them to understand who has their data, what was collected, if it can be deleted, and how they can opt-out of downstream selling. Today, as we battle a pandemic that has moved so much of life online, companies now know more about us, our children, and our habits. Massive amounts of data are collected that reveal everything from what's inside the packages delivered to our door, to what food we ordered for dinner, and what TV programs we stream in the evening, to even more sensitive information like whether and how we are

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029

trying to start a family and what our financial condition is. This data is collected and sold, and potentially used in decisions businesses make about you, as well as your access to credit, employment, or even healthcare.

As Congress and your committee consider federal legislation to advance much-needed privacy rights to consumers across the country, it is important that no such legislation preempts the important work that is happening at the state level. States are the laboratories of democracy. I ask that, at the very least, the federal government respect the role of the states here and not undermine our work by seeking to broadly preempt our laws.

I encourage the members of the committee to favor legislation that sets a federal privacy-protection floor rather than a ceiling, allowing my state and others that may follow the opportunity to provide further protections tailored to our residents. Any federal legislation should leave in place more protective state laws, a model that Congress has employed in other consumer protection legislation, including laws relating to children's privacy and health privacy, and laws that enable a federal baseline with states making decisions about additional protections for their jurisdictions.

California welcomes a partner with the tools and resources for vigorous enforcement of new consumer privacy rights. Any proposal that Congress crafts should guarantee privacy rights for consumers and include a meaningful enforcement regime that respect the good work undertaken by states around the country. I invite Congress to look to the states as sources of nimble innovation and expertise in data privacy, and to value protections, like the CCPA, that states have already developed.

Thank you.

1300 I Street • Suite 1740 • Sacramento, California 95814 • (916) 210-6029