

CONSUMER PROTECTION POLICY CENTER

consumeraction





September 7, 2022

The Honorable Nancy Pelosi
Speaker of the House of Representatives
1236 Longworth H.O.B.
Washington, DC 20515

RE: Federal Preemption of California's Landmark Privacy Law

Dear Speaker Pelosi,

We wish to thank you for your commitment to protecting privacy rights in California with your recent remarks regarding the American Data Privacy and Protection Act (ADPPA). As organizations committed to personal privacy, reproductive rights and democracy, we urge you to prevent federal preemption of California's landmark privacy law, the California Consumer Privacy Act (CCPA), enacted in 2018 and strengthened by voters in 2020 with the California Privacy Rights Act (CPRA).

US privacy laws have a long history of setting a floor, not a ceiling, on protections. Yet the ADPPA would needlessly take away existing rights from 40 million Californians. The bill will exempt companies that provide data to government agencies, leave the law vulnerable to weakening by industry lobbyists, and swiftly cancel years of progress in California. The reach of these changes is profound, impacting everything from immigration rights to freedom of assembly. It will also handicap the fight for abortion rights.

Critically, California's law protects against government surveillance. A major loophole in the ADPPA allows companies who contract with government entities for data collection to avoid its

protections. In contrast, under California law, companies that contract with the government are covered businesses that must comply with the law. Sensitive personal information residents choose to protect from companies and the government under the CCPA would be exposed under the ADPPA. That means unfettered access by governments to mass data collection by tech companies like Google.

Once data gets into other hands, it goes everywhere and is hard to track. Purchasing data is one way governments circumvent the constitutional protections that require them to seek judicial approval through warrants before they violate our 4th Amendment rights against unreasonable searches.

This is already happening across the country. A location data company called SafeGraph collected information on those who go to abortion clinics and put it up for sale on the open market. That information could have been purchased by anyone, including anti-abortion vigilante groups or police.

But, under California's law, any resident who exercised their opt-out choice is protected from a government's extra-judicial purchase of their private information. ADPPA would overturn that protection.

Or take the example of a woman traveling to California for an abortion from an anti-choice state. Under the ADPPA, the sheriff in her hometown can put Big Data to work to deter out of state abortions. He can contract with a company to flag a woman's searches for abortion clinics by monitoring search traffic, flag her travel purchase to an abortion access state, and collect location information when she arrives at the doctor's office in California. Those who helped her could be prosecuted, including her local doctor and mother. The California doctor she saw could be exposed to prosecution if the doctor traveled to her home state, because a Californian's ability to prevent their information from being sold to any government – including that anti-choice sheriff – is stripped by the ADPPA. Meanwhile, anti-choice states are trying to pass legislation to criminalize out-of-state abortions.

Because of the federal loophole people across the nation will not be able to make reproductive choices privately and even Californians will become easier targets for criminal prosecution.

It's not just the battle for reproductive rights that will be in danger. Communities of color, low-income workers, immigrants, the LGBTQ community, and marginalized people everywhere will be disparately impacted by the loophole that allows the government to monitor their every move.

U.S. Customs and Border Patrol has weaponized personal data to devastating effect[1]. Palantir, the largest data analytics company in the world, has contracted with the Department of Homeland Security to conduct immigration raids[2]. Other branches of the government, such as the

[1] "Ice is Buying Up Massive Troves of Location Data…For Some Reason," Nikki McCann Ramirez, Rolling Stone, July 18, 2022, https://www.rollingstone.com/politics/politics-news/ice-dhs-privacy-location-data-aclu-1384797/
[2] "The war inside Palantir," Doug MacMillan, The Washington Post, August 22, 2019, https://www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees/

FBI and DEA, have contracted with the data broker Venntel, which purchases data from another company, Mobilewalla, that covertly monitored the location and identity of almost 17,000 people who assembled during the Black Lives Matter protests in 2020[3]. The CCPA allows Californians to opt out of this location surveillance, but preemption will allow companies to use the loophole.

Another critical strength of the CCPA is that lawmakers cannot weaken its protections without the consent of voters. That means privacy in California has nowhere to go but up. ADPPA's preemption sets a ceiling on privacy protections that no state may exceed, and would allow Congress to weaken or even eliminate those protections at any time.

All Americans deserve privacy protections, but preemption is a false choice pitting California's law against protections for all Americans. We can have both. Strong federal privacy laws already co-exist with stronger state privacy laws. The Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Electronic Communications Privacy Act all established national policy "floors" and let states enact more privacy-protective legislation.

California's law takes full effect in a few months, but rules implementing much of the ADPPA will take two years to be written by the FTC. Delay is denial. The delay, and rollback of stronger state protections, is welcomed by tech companies who don't want to comply with California's law.

California also offers more protection against coercive pricing when consumers exercise their privacy rights. The state's law prohibits such charges from being "unjust, unreasonable, coercive or usurious" and requires companies to prove a different price for those who choose privacy is "reasonably related to the value provided to the business by the consumer's data." ADDPA would override these provisions.

California's law creates a right to opt-out of profiling and automated decision-making, allowing consumers to prevent discrimination in access to jobs, housing, loans, etc. that occurs when biased algorithms go to work and ignore civil rights. This broad opt-out from automated decision-making is in some ways more protective than the ADPPA's bar on racial discrimination, because the ADPPA relies on companies to decide if their algorithms are biased. California's law will allow consumers to simply say, "Don't profile me at all."

And while amendments to ADPPA nominally allow California to enforce the law, the privacy board cites "significant uncertainties" in its ability to do so.

The California Privacy Protection Agency, charged with enforcing our state law, Governor Gavin Newsom, Assembly Speaker Anthony Rendon, Attorney General Rob Bonta, and numerous other state and federal lawmakers have expressed the same objections to preemption.

---

[3] "How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies," Byrin Tau, The Wall Street Journal, https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202

We urge you to ensure the important privacy protections for all residents contained in the ADPPA do not come at the expense of the robust law Californians have already enacted.

Sincerely,

Consumer Action
Children's Advocacy Institute
Consumer Protection Policy Center
Consumer Watchdog
Privacy Rights Clearinghouse

cc: California Congressional Delegation