California Wants to Stop Data Brokers From Selling Your Information. Congress May Follow

May 24, 2026 - California is taking one of the country's most aggressive steps against the growing business of buying and selling Americans' personal information, but privacy advocates warn the state's effort only works if consumers actively participate - and even then, major loopholes remain. Beginning in this year, California residents will be able to use a system called DROP, short for Delete Request and Opt-Out Platform, to demand that registered data brokers delete personal information collected about them. The DROP platform is already taking registrations but enforcement doesn't begin until August.

The California Privacy Protection Agency says the system is designed to make it easier for consumers to stop companies from trading information such as location history, browsing habits, app usage, shopping activity, and other personal data.

Supporters say the effort is important because data brokers have quietly built a multibillion-dollar industry around collecting and packaging detailed consumer information. That data can then be sold to advertisers, private companies, political organizations, and in some cases government agencies. DROP represents a real threat to these practices, but consumers need to understand that California's protections have limits.

First, the law primarily applies to brokers doing business in California or handling California consumer data. It does not automatically prevent companies outside California from collecting or selling information through other channels.

Second, the law does not automatically erase anyone from broker databases. Consumers must actively register and submit requests through the DROP system for the protections to take effect.

Without taking that step, Californians may still have their information circulating through commercial databases that can potentially be purchased by buyers in other states or by federal agencies.

That concern has become part of a larger national debate over what critics call the "data broker loophole."

The issue centers on whether law enforcement and intelligence agencies should be allowed to buy Americans' commercial data without first obtaining a warrant. The House Appropriations Committee has now advanced language in the federal Commerce-Justice-Science appropriations bill that would restrict agencies funded under the bill from purchasing certain commercially available personal information from data brokers unless they obtain a search warrant first.

The proposal has drawn support from some conservative lawmakers, civil-liberties advocates, and privacy organizations that argue the government should not be able to purchase information that would otherwise require a court order to obtain directly. The provision is tied to the annual Commerce-Justice-Science funding bill, which covers agencies including the Department of Justice and the FBI. It is not part of the Department of Homeland Security appropriations process and is not currently moving through budget reconciliation rules that allow certain Senate legislation to pass with a simple majority.

That means the proposal still faces several political hurdles.

The full House must approve the spending bill. The Senate would then need to negotiate its own version, and lawmakers from both chambers would have to reconcile differences before any final measure could become law. At the moment, there is no indication the Senate has formally adopted the House language.

The proposal also mirrors broader legislation known as the Fourth Amendment Is Not For Sale Act, which has been debated in Congress for several years but has not yet been fully enacted.

Even if the current proposal survives, privacy advocates say it would only address one part of the government's expanding surveillance capabilities.

The legislation focuses specifically on agencies purchasing commercially available data from brokers. It does not eliminate other forms of government surveillance, including subpoenas, warrants, geofence requests, social media monitoring, or data voluntarily shared with private companies.

It also would have limited impact on the Foreign Intelligence Surveillance Act, commonly known as FISA.

Under Section 702 of FISA, intelligence agencies can collect communications involving foreign surveillance targets located overseas. Americans can still be swept into those collections incidentally if they communicate with foreign targets or appear in related intelligence gathering.

Critics have long argued that federal agencies increasingly combine traditional surveillance powers with commercially purchased data to build broader pictures of Americans' activities and relationships.

The proposed appropriations language does not repeal or significantly alter Section 702 authorities. But if passed, it would limit one additional path agencies may use to gather information - purchasing it directly from commercial data sellers.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS