# Congress Considering National Privacy Law That Could Significantly Weaken Stronger State Protections

May 29, 2026 - Congress is once again attempting to create a national consumer privacy standard, but the latest proposal could weaken some of the strongest protections Americans currently have rather than strengthen them. The proposed SECURE Data Act would establish federal rules governing how companies collect, share, store, and use personal information. Supporters say the bill would simplify compliance requirements for businesses operating across multiple states and provide nationwide consumer protections. But privacy advocates argue the bill's broad federal preemption language - often called a usurpation clause by critics - could override stronger laws in several states, especially California's.

That concern is drawing increasing attention because California is preparing to launch one of the country's most aggressive consumer privacy tools: the Delete Request and Opt-Out Platform, known as DROP. Beginning August 1, California residents will be able to submit a single deletion request through DROP and require hundreds of registered data brokers to delete personal information they have collected. Instead of forcing consumers to contact companies one by one, the system centralizes the process through the California Privacy Protection Agency.

For consumers, the practical impact could be significant. Data brokers collect and sell information tied to browsing activity, shopping habits, geolocation, household income, property ownership, and other highly personal details. California's DROP system is designed to give consumers a realistic way to claw back some control over how that information is distributed.

The concern about what Congress is working on is that a national law could override separate enforcement structures or eliminate state-specific requirements that go beyond federal standards. DROP would likely be a victim of such a law it preempts state laws. And there are a lot of groups lobbying for that type of preemption.

The debate cuts to the center of a larger question: whether Congress is trying to establish a minimum national privacy baseline or a maximum ceiling that prevents states from adopting stronger protections.

The bill's title itself has also drawn skepticism.

Calling legislation the SECURE Data Act is difficult to justify if consumers still lack meaningful control over how their personal information is collected, sold, profiled, and retained. Data is not truly secure simply because companies disclose their practices in lengthy privacy notices that few consumers read or understand, and if consumers don't have some meaningful way of managing that data.

The proposal does include provisions allowing consumers to correct inaccurate personal information. But Americans have heard similar promises before.

The Fair Credit Reporting Act has included dispute and correction rights for decades. In practice, however, many consumers have found correcting inaccurate credit information to be slow, frustrating, and heavily tilted in favor of large credit reporting agencies. Errors can take months to resolve, disputes are frequently rejected with little explanation, and consumers often must repeatedly submit documentation to fix mistakes affecting loans, insurance rates, or employment opportunities. Simply placing correction language into a federal privacy bill does not guarantee consumers will have meaningful or practical control over their data.

If Congress chooses to focus on establishing a national minimum privacy standard instead of overriding tougher protections already enacted by states, that would be a good thing. Under that approach, federal law would guarantee baseline rights nationwide while still allowing states such as California to adopt additional protections when new technologies or data practices emerge.

It is worth noting that state experimentation has historically driven consumer protections forward. California's privacy laws, including the CCPA, CPRA, and DROP program, have become models influencing legislation across the country. Preempting these laws may be supported by businesses, but that would do a great disservice to the general public.

For now, the SECURE Data Act remains in the early stages of the legislative process and has not passed Congress. But the fight over federal preemption may ultimately determine whether Americans gain stronger privacy rights - or lose a variety of much stronger state protections they already have.

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