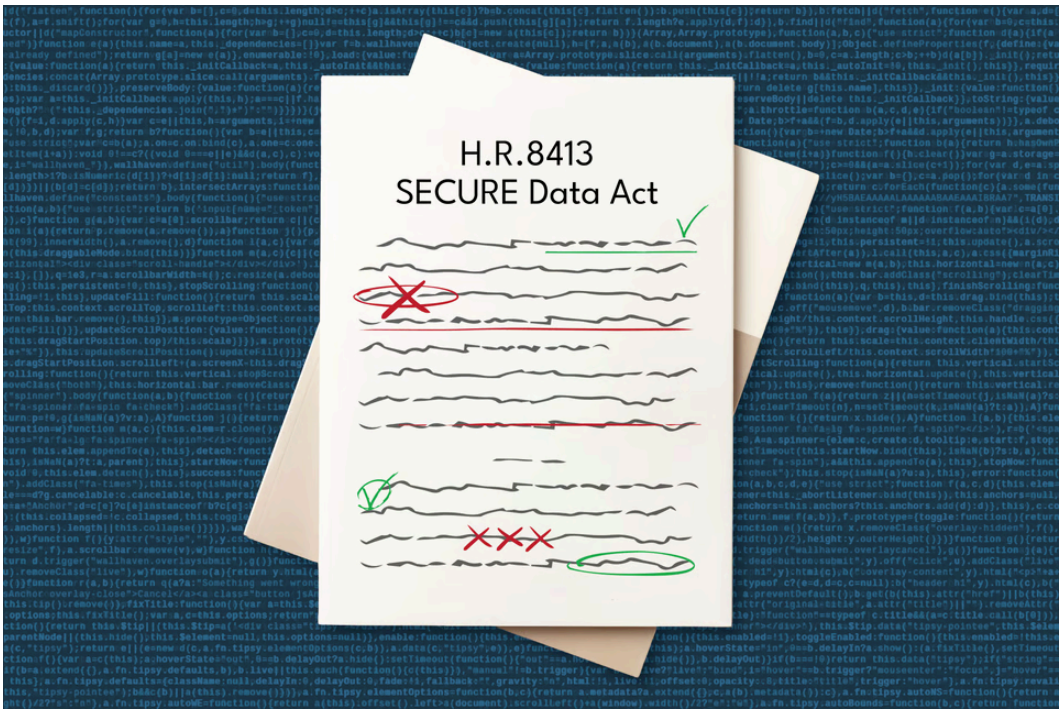
BLOG *Published June 3, 2026 · 9 minute read*

New Data Privacy Legislation is a Good Start. Here's How to Make It Better.

Ruth Whittaker



Every minute, Americans hand over intimate details of their lives—where they go, what they buy, who they talk to, what they search for—with little control over where that data ends up. Yet despite years of debate, Congress still has not enacted basic nationwide privacy protections. As Washington dithers, states have filled the gap, creating a growing patchwork of rules that leaves consumers unevenly protected and forces businesses to navigate different standards across the country.

Enter the SECURE Data Act. This bill, introduced by Rep. John Joyce (R-PA) on behalf of the Data Privacy Working Group, is a Republican-led proposal to create nationwide privacy protections and a uniform federal standard. The bill is not perfect, but it is a serious starting point. It includes several provisions with bipartisan appeal, including individual privacy rights, sensitive data protections, and a national data broker registry. But it also needs major improvements before it can become a durable federal framework, like stronger enforcement, narrower preemption, and better tools for consumers.

As lawmakers work to enact real privacy protections, we've highlighted five things policymakers should like in the bill and five big things they need to fix.

5 Things to Like in the SECURE Data Act

1. It's Comprehensive

The United States is one of the only major economies without comprehensive protections for personal data. In the absence of federal action, consumers and businesses must navigate a growing patchwork of state-level rules. Meanwhile, the most sensitive information we have—our precise locations, genetic codes, browsing patterns, and health stats—are collected, bought, and sold on secondary markets, often without our knowledge or consent.

Bipartisan work on privacy has stalled since the American Privacy Rights Act failed to move out of committee in 2024. The fact that Congress has a comprehensive framework up for consideration again is a promising start.

2. It Gives Consumers Core Privacy Rights

The individual rights outlined in the bill align with best practices from states and previous bipartisan federal work. It gives consumers the right to know what data is collected, delete or correct it once it's collected, and know who it's shared with. It also lets people opt out of targeted ads and sales to data brokers, limiting how third parties can profit from personal information.

The bill also recognizes that some data is more sensitive and needs more protection. It prohibits data collectors from processing sensitive data—like racial information, health diagnoses, and precise geolocation data—without getting permission first.

Together, these rights would give people real control over their data.

3. It Makes Compliance Easier to Navigate

Data privacy is complicated. A comprehensive framework would affect nearly every industry in the modern economy. An effective framework can't just expand individual rights—it must also give businesses a clear way to comply with the law.

This bill makes a serious effort to reduce complexity, especially for small businesses. It tasks the Department of Commerce with developing a small business compliance guide and lets larger companies work together to develop codes of conduct specific to their industries in order to navigate the new rules.

Creating those guides, and making them available to the public for review, would cut down on confusion for businesses and give consumers more clarity about how their data is handled once it's collected.

4. It Lays the Groundwork for One-click Control

The rights laid out in the bill only matter if consumers can realistically use them. Expecting consumers to set their preferences for every website, app, or device they encounter would quickly become overwhelming and ineffective. When was the last time anyone paid attention to a cookie banner or read through a privacy policy?

To reduce that complexity, the bill commissions a study of a universal opt-out mechanism: a single portal for consumers to set their data preferences across the entire internet. If implemented, this tool would save consumers time and help them exercise their rights. It would also give data collectors a clear, consistent signal about what consumers want.

5. It Brings Transparency and Accountability to Shady Data Brokers

Data brokers collect, aggregate, and sell huge amounts of personal information, often without people knowing they exist. The data they sell can impact everything from insurance rates to credit eligibility and, if breached, can create serious privacy and security risks.

Drawing inspiration from California, this bill would create a national data broker registry to shed light on this shadowy industry. Brokers would have to disclose the categories of data they sell, how they vet potential buyers, and document any instances of unauthorized data access. The registry would also be available to the public, giving consumers visibility into the entire data ecosystem, not just the point of collection.

5 Things to Fix in the SECURE Data Act

1. Significantly Improve Enforcement

The enforcement mechanisms in this bill are far too weak. The current draft gives violators 45 days to address alleged violations before enforcers can act. It also allows industry to pick their own watchdogs and builds in nearly a full year of delays before noncompliant practices need to be changed. Taken together, these policies tie enforcers' hands even when consumers face serious harm.

Some advocates have called for a "private right of action," which would allow individuals to sue when their rights are violated. But partisan lines are already being drawn over the issue. [1] Short of including a private right of action, there are other ways to give the bill real teeth.

First, the "right to cure" should be changed. The current draft would give companies a 45 day "cure period" to fix alleged violations on their own before enforcers can take them to court. Lawmakers should shorten the duration of the cure period and make the proposed cures subject to judicial review. For egregious or willful violations, the cure period should not apply. A company accused of ignoring consumer preferences and selling their sensitive data without consent shouldn't be granted 45 days to come up with their own solution—enforcers should be able to take immediate action.

Second, the safe harbor provisions for large companies participating in a code of conduct should be eliminated. Right now, companies who simply participate in a code of conduct are given a built-in legal defense, a "rebuttable presumption," that makes it harder for enforcers to take them to court. The goal of the codes of conduct should be to guide industries through complexity, not to create a legal shield against accountability.

2. Shed Light on Data Sales

While the individual rights laid out in the bill would go a long way in making the data ecosystem more transparent, they could go even further. For example, the bill only requires data collectors to share the "categories" of third parties with whom they share data, even when that includes sales or transfers consumers might not expect. That could leave

consumers with only broad labels rather than meaningful information about where their data goes.

Data collectors should have to name the individual third parties to whom they sell consumer data. Combined with the data broker registry, named disclosures would allow consumers to follow their data across the entire ecosystem and make targeted decisions about which parties they trust and when they need to opt out.

3. Protect Teens' Privacy and Autonomy

Ironically, the current draft of the bill could leave internet users aged 13-16 with less privacy than they have today. The bill is right to treat minors' data as sensitive. But the current draft also undermines teens' ability to control their own data. Unlike other child-focused privacy proposals, this bill would give parents the exclusive right to view, amend, and delete teens' information. That means a 16-year-old could have their online identity, including information about their gender identity or sexual orientation, reviewed and even changed by a parent without their knowledge or consent.

Children do need more protection online, and parents have an important role to play in setting appropriate privacy standards. But older teens also have a reasonable expectation of privacy and should be given more autonomy to control their online lives. A bill meant to protect teens should not undermine their privacy rights.

4. Don't Make Consumers Wait for a Universal Opt-out

The study of the universal opt-out mechanism is a great start. But while that study is ongoing, consumers shouldn't have to fend for themselves. Many states, including California and Texas, already allow consumers to use browsers, extensions, or other third-party tools to send privacy signals automatically. [2] These tools save consumers time and give them meaningful control over their data.

To be sure, it would be much easier for consumers and businesses to communicate with a single entity. The ultimate goal should be to implement the universal opt-out mechanism. But while the technical details and logistics are being studied, policymakers could temporarily allow consumers to use third-party shortcuts.

5. Don't Gut Consumer Protections When Preempting State Laws

Any comprehensive privacy bill with robust protections should replace the confusing patchwork of state privacy laws with a single standard. But the SECURE Data Act's preemption language could be overbroad.

Because the bill blocks state laws that "relate to" its provisions, it could be interpreted to reach beyond comprehensive privacy laws and sweep in narrower protections, including cybersecurity standards, data breach claims, children's privacy rules, and health data protections. [3] For example, because the bill imposes cybersecurity standards on data collectors, it could make it harder for people to bring common law claims after data breaches. [4]

Creating a single set of privacy rules is important. But it must be carefully crafted to avoid unintentionally sweeping in other consumer protection laws or creating legal uncertainty.

Conclusion

The SECURE Data Act gives Congress a real chance to restart the privacy debate. Its core structure is workable: national rights, clearer rules for businesses, and new transparency for data brokers. But to succeed, the bill needs stronger enforcement, more usable consumer controls, better protections for teens, and a narrower preemption clause. With those fixes, Congress could finally move from years of debate to delivering the meaningful privacy protections Americans deserve.

ENDNOTES

1. Bordelon, Brendan and Alfred Ng, “Democrats’ federal privacy wishlist”. *Morning* Tech newsletter, PoliticoPro, 5 May 2026. https://subscriber.politicopro.com/newsletter/2026/05/democrats-federal-privacy-wishlist-00905952. Accessed 27 May 2026.

2. Pringle, Jack. “Opt-out Signals no Longer Just Noise: State Privacy Law Requirements Taking Shape”. Nelson Mullins Riley & Scarborough LLP, 7 Oct. 2024. https://www.nelsonmullins.com/insights/insights/opt-out-signals-no-longer-just-noise-state-privacy-law-requirements-taking-shape. Accessed 27 May 2026.

3. Francis, Jordan et al. “Contextualizing the Proposed SECURE Data Act in the State Privacy Landscape”. Future of Privacy Forum, 23 April 2026. https://fpf.org/blog/contextualizing-the-proposed-secure-data-act-in-the-state-privacy-landscape/. Accessed 27 May 2026.

4. Carlin, John P. et al. “The SECURE Data Act: A New Federal Policy Framework”. Paul, Weiss, Rifkind, Wharton & Garrison LLP, 28 April 2026. https://www.paulweiss.com/insights/client-memos/the-secure-data-act-a-new-federal-privacy-framework. Accessed 27 May 2026.