



## **Policy Proposal: A Federal Privacy Standard**

*Published: April 23, 2026*

***Every American should have the right to control and protect their personal information. Advertisers, fraudsters, identity thieves, foreign adversaries, and even our own government are constantly looking to access and use our personal data. A well-constructed federal privacy policy would protect consumers and stimulate innovation – a no-brainer win-win.***

### ***Why is protecting personal data so important?***

The combination of massive amounts of data being collected about each of us with lax security implementation and no federal privacy standards leaves all of us vulnerable to bad actors and abusive practices.

Did you know your car insurance rates may be based in part on individual driving behaviors collected without your knowledge?

Did you know that health insurance companies get insights on consumers that are based on things like daily step counts, heart rate, and calorie intake, all taken from wearable devices?

How do you feel about targeted anti-abortion ads being sent to people who had visited ~600 different Planned Parenthood locations?

And those are just “legitimate” use cases for data.

Frequent leaks and theft of our sensitive information allow criminals to fraudulently charge things to our debit/credit cards, take over our email and social media accounts, or attempt to apply for credit/loans in our name. In fact, one poll found that 34% of Americans – that’s 1 out of every 3 – had experienced one of these three issues in just the past year.

Meanwhile, 71% of Americans are concerned about how the government uses their data.



### ***So Americans want more regulation to protect their data?***

They do – 72% think there should be more government regulation of what companies can do with customers’ personal data. Which makes sense given that a majority (61%) are skeptical that anything they do today will make much difference when it comes to protecting their personal information and only 21% are confident that those who have access to their personal information will do what is right.

### ***Aren’t states already regulating personal data and isn’t that enough?***

Today, 20 states have passed their own privacy laws.

There are several problems with that.

First, while it’s great that residents of places like California, Colorado, Connecticut, and Delaware are protected by comprehensive data privacy laws, it’s less great that residents of places like Maine, Michigan, Nevada, and New York are only protected by narrow data privacy laws, and it’s not great that residents of places like Arizona, Idaho, New Mexico, and Wyoming have few, if any, protections. That’s to say nothing of people who travel from one state to another and have no idea what protections they are covered by when in a new place.

Second, the patchwork of state-level regulations makes it difficult on businesses, as they are forced to comply with myriad different standards and be prepared for even more (since 2018, 46 states have introduced 210 different privacy laws). Increased costs are bad for companies/consumers; innovation suffers when investments scale less efficiently.

### ***Have other countries/regions experimented with privacy regulation?***

They have - the European Union’s General Data Protection Regulation (GDPR) is one of the most well-known and well-researched, from which we can learn a great deal.

### ***What would a federal privacy standard look like?***

A federal privacy standard would have to replace the patchwork of state laws that currently exists. There is still ongoing discussion and debate about whether a federal standard should *replace* state laws or should set a *floor* that states are able to build upon. That question requires further consideration.



Privacy standards should have a higher level of protection applied to particularly sensitive or high-risk data – for example, in Europe, sensitive personal data includes racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic data, etc.

Data holders should have minimum data security standards applied to them with rigorous monitoring and enforcement.

Limits should be placed on the sale/transfer of data to third parties.

Users should have knowledge and control over what data is collected.

And consistent standards for data collection, storage, and use should be established.

***Republicans have just introduced a new bill - H.R. 8413, the SECURE Data Act; is that the answer?***

Unfortunately, it is not; just how supportive big businesses have been of the bill should give consumers some sense of how poorly they'll fare under it.

The actual privacy standards are relatively weak and omit many of the most critical consumer concerns (e.g., requirements to affirmatively minimize collection of data and bans on selling certain sensitive information).

The lack of a private right of action is also glaring hole – instead enforcement would rest with the FTC and state attorneys general, with no recourse in court if those entities fail to serve as effective advocates.

The strict preemption regime is a real, reasonable, concern to residents of states that have opted for more robust privacy regimes given the concerns above.

Other, previous, bills, like the American Data Privacy and Protection Act and the American Privacy Rights Act better addressed the needs of consumers.



***Would a federal privacy standard impact other ongoing debates?***

It would – for example:

- Age assurance technologies (where platforms limit content/services available to children) would be less controversial if the data used to implement them were better protected
- Social media protections currently available only to children under the age of 13 could be made more easily available to older kids, mitigating some of the harm they currently experience when using those tools
- And, of course, artificial intelligence opens a whole can of worms on data protection, which we'll address separately.

***Every day Americans suffer the consequences of having their personal data stolen or sold without their knowledge or consent. While Rep. Clarke takes money from corporations and PACs attempting to minimize consumer protections, I'm proud to advocate for a federal privacy standard that protects consumers and small businesses, fosters responsible innovation, and treats all Americans as people, not bits of data.***

Sources include:

- <https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/>
- <https://oercs.berkeley.edu/privacy/selected-privacy-policies-and-regulations/international-privacy-laws>
- <https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#states-with-comprehensive-data-privacy-laws>
- <https://yougov.com/en-us/articles/52425-what-americans-think-about-privacy-united-states-government-surveillance-in-2025-poll>
- <https://www.technet.org/privacy/>
- <https://www.businessroundtable.org/business-associations-welcome-federal-data-privacy-legislation>
- <https://iapp.org/news/a/secure-data-act-analysis-of-the-new-federal-privacy-bill>
- <https://www.fisherphillips.com/en/insights/insights/house-republicans-unveil-national-data-privacy-bill>
- <https://www.hunton.com/privacy-and-cybersecurity-law-blog/house-republicans-introduce-comprehensive-federal-privacy-bill-secure-data-act>
- <https://www.thirdway.org/memo/privacy-please-data-privacy-should-be-tech-priority-number-1>