A Patchwork Of State Laws Is The Wrong Approach To Privacy Regulation

IA members support a nationwide comprehensive privacy law that empowers consumers, increases transparency, and provides Americans with meaningful control and the ability to access, correct, delete, and download the data they provide to companies.

States are continuing to advance privacy laws in the absence of a comprehensive federal privacy bill. During the 2020-2021 legislative sessions, 28 states across the country introduced, came close to passing, or passed, state-specific consumer privacy bills, expanding the patchwork of state privacy laws from coast to coast. These inconsistent state rules not only confuse consumers but also increase risk and costs for Americans businesses.

Twenty nine states passed laws related to data privacy, creating a patchwork of protections in the U.S.

- **California** passed by ballot measure the California Privacy Rights Act (CPRA), which expanded the California Consumer Privacy Act (CCPA), which only became effective in 2020. The CPRA changed important definitions in the law, expanded the law's scope, and created a new enforcement agency with broad regulatory discretion.
- **Virginia** passed the Consumer Data Protection Act (CDPA), which includes Virginia Attorney General enforcement.
- **Colorado** passed the Colorado Privacy Act (CPA) does not include an outright exemption for companies subject to HIPAA, and includes an unclear global browser opt-out provision.

The patchwork of state privacy laws has only become more complex during the 2020-2021 state legislative sessions.

4 states have passed comprehensive consumer privacy laws that do not align with each other.

5 states considered privacy bills related to location data.

8 states introduced COVID-19 data or contact tracing bills.

4 states considered legislation around facial recognition.

15 states held hearings or roundtables to discuss state comprehensive privacy bills.

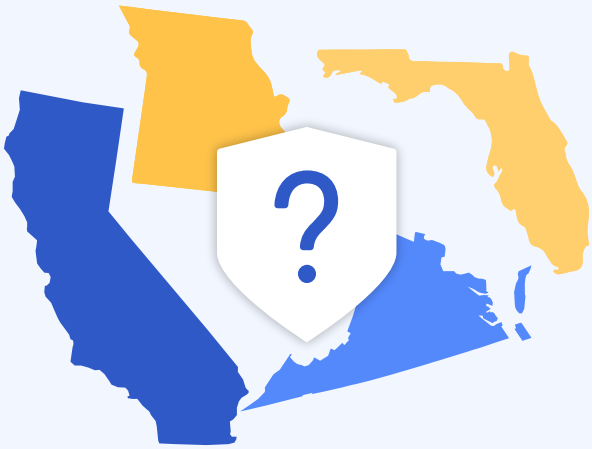
Consumers and businesses lose out when states take different approaches to privacy legislation. Laws conflict and cause consumer confusion for interstate transactions.

When these laws become effective, companies may be required to comply with four different sets of state privacy regulations from California, Colorado, Nevada, and Virginia. These state laws are in addition to any already existing sector-specific federal (like laws governing financial services and medical providers) or state laws (like Maine's law for internet service providers). The burden of complying with the patchwork of state laws is especially difficult for small and medium sized businesses just starting out. Because states have inconsistent rules regarding consumer privacy, more individuals' personal data may end up being collected than if a comprehensive nationwide privacy bill was enacted.

It is likely that more comprehensive state privacy laws will pass in the near future, only adding to the confusion. The longer Congress takes to establish a national standard for privacy protections, the greater the probability that small and medium sized businesses will struggle to comply with the ever-changing state privacy law patchwork.

State laws do not provide consumers with consistent privacy protections.

Starting in 2023, an app developer, for example, has to comply with at least four different sets of privacy standards if they want their products or services used nationwide.



Expectations about your privacy protections should not change based on where you live.

Congress should embrace the bipartisan nature of privacy legislation in order to pass a comprehensive federal privacy law that truly protects all Americans.

About Internet Association

Internet Association represents over 40 of the world's leading internet companies. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. For more information, visit *www.internetassociation.org*