In-House Counsel
Oct. 11, 2023, 2:00 AM PDT

Varied Data Privacy Laws Across States Raise Compliance Stakes

By Brenna Goth

- States target consumer data, health privacy
- Patchwork expands with differing mandates

Companies are navigating an increasingly complex set of laws for how they collect and use personal information as states diverge in their approaches to boosting data privacy standards.

Lawmakers across the country are pushing for more oversight over how businesses treat consumer data that can be linked to an individual and used to profile them or target them with advertising. The US does not have a comprehensive federal data privacy law, which has spurred state action.

Thirteen states have now enacted broad consumer privacy laws to give people more control over their data, a count that more than doubled this year. A handful have also approved new safeguards specifically for health data and for the data of kids and teens. The number is expected to grow in the new year.

The pace of adding new laws to the patchwork means the US state privacy landscape is rapidly changing, and compliance has become more difficult across a variety of industries. While some of the laws are similar in structure, each has its own nuances, such as how certain categories of data are defined.

“One of the biggest compliance challenges is just having to adhere privacy practices to the myriad of different approaches that states are adopting,” said Howard Waltzman, partner at Mayer Brown LLP who co-leads the public policy, regulatory, and government affairs group.

For individuals, their data privacy rights differ largely depending on which state they reside. That determination is an additional challenge for businesses.

“It’s a nightmare trying to evaluate: is this where somebody lives, is this where somebody works, or is this where somebody’s just visiting?” Waltzman said.

Differing Requirements

Broad consumer privacy laws require that companies disclose how they collect and use data, as well as give individuals the right to access that data or limit its use.

The statutes differ in their scope and some of their specifics. A Florida law, for instance, targets large tech companies while requirements in other states apply more broadly to a larger swath of businesses.

A few states cover nonprofit organizations in addition to companies. California goes beyond laws elsewhere by including employee and business-to-business data.

Companies taking a uniform approach across states may make compliance simpler, but can come with trade-offs for other parts of their business. Businesses may not necessarily want to apply the most stringent approach—or the highest common denominator of privacy regulations—across an entire organization, said Corey Dennis, US privacy officer at the healthcare company Sanofi.

California can be a good model for companies that want to set up broad privacy compliance, said Christina Ayiotis, associate general counsel for cybersecurity and privacy at Lumen Technologies. The Golden State is widely recognized as having the most rigorous state privacy requirements, and companies are likely to have a lot of business there, she said. California is the biggest US state by population with 39 million people.

“I think businesses need to do an analysis and figure out, ‘Should we just go ahead and try and meet those requirements for everyone, even though people in non-California states don’t have the rights like the California residents do?’” she said.

Companies can benefit from a holistic approach to privacy compliance that looks at both the similarities and differences in the laws, said Cinthia Granados Motley, director of the global data privacy and information security practice group at Dykema Gossett PLLC. Businesses have a head start for the new laws going into effect if they’re already following the EU’s General Data Protection Regulation or California’s data privacy law, she said.

“Now it’s just kind of continuing to monitor the state laws coming up and seeing what additional tasks need to be done to integrate that into what hopefully companies will have already as a privacy compliance program,” she said.

Notably, the laws also focus on transparency, Motley said. Companies need to make it clear to their customers how they are collecting and using data.

“You will find that these laws, simple or onerous, go after that, meaning you can’t bury your privacy policy anymore like in the past,” she said.

Health Data Targeted

Company executives should also take note of a first-in-the-nation law regulating consumer health data in Washington state. Legislators elsewhere also prioritized boosting protections for health data this year.

The Washington My Health My Data Act is notable for its private right of action to bring lawsuits, broad scope, and onerous obligations, said Ieuan Jolly, partner at Linklaters LLP. The bulk of the law will go into effect in March and June 2024.

“The private right of action has a lot of teeth behind it,” he said.

The law’s requirements include that companies obtain consent to collect consumer health data that can be linked to physical or mental health status. Health apps that track digestion, for instance, would fall under the law, as would information used to infer if a consumer is pregnant, according to the Washington Attorney General’s Office.

The privacy and online safety of youth also drew state lawmaker attention this year, but ongoing litigation raises questions over the future viability of such legislation. Legislators who argue youth need additional protections have differed in their policy approach.

States including Delaware and Connecticut will heighten requirements for the collection and processing of minors’ data as part of their broader consumer privacy laws. Meanwhile, Utah and Arkansas have focused more narrowly on social media platforms, including to require parental permission for youth under 18 to open accounts.

Other states have looked at California’s approach to require websites likely to be accessed by children to follow stricter privacy and design standards. Federal judges, however, halted both the California and Arkansas laws with preliminary injunctions in litigation raising First Amendment concerns brought by tech companies.

— With assistance from Isabel Gottlieb.

To contact the reporter on this story: Brenna Goth in Phoenix at bgoth@bloombergindustry.com

To contact the editor responsible for this story: Bill Swindell at bswindell@bloombergindustry.com

Related Stories

Delaware Sweeps In Nonprofits, Kids’ Data In Digital Privacy Law
Sept. 20, 2023, 2:00 AM PDT

States Ready To Reboot California-Style Kids’ Privacy Proposals
Sept. 6, 2023, 2:00 AM PDT

Abortion-Rights States Begin Shielding Digital Data Near Clinics
July 24, 2023, 2:05 AM PDT

Connecticut Is Latest State To Broaden Its Online Privacy Law
July 7, 2023, 2:00 AM PDT

DeSantis Takes Swing At Big Tech In New Florida Privacy Law (1)
June 6, 2023, 9:28 AM PDT

More Stories (1)