State Net®

State Leadership on Data Privacy Creating Regulatory Patchwork

By Korey Clark, Editor, State Net Capitol Journal™

In the absence of comprehensive federal legislation addressing data privacy, state legislatures have taken matters into their own hands, introducing data privacy measures in increasing number each year and enacting many of them into law. The surge of legislation, ranging from piecemeal efforts addressing specific areas of data privacy, such as biometric or genetic data, to comprehensive measures, is creating headaches for government affairs and compliance professionals alike, particularly those tasked with keeping tabs on multiple jurisdictions.

States Step into Federal Legislative Gap on Data Privacy

Few issues galvanize Americans' concerns about the ubiquity of technology in our daily lives more than data privacy. An overwhelming majority (84%) say they are at least somewhat concerned about the safety and privacy of the personal data they provide on the internet and more than one-third (37%) say that personal data they have provided online has been compromised, according to a 2022 Ipsos survey.

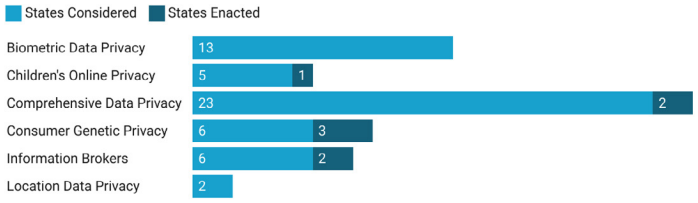
And yet the U.S. Congress has done very little to enact national legislation establishing guidelines for collecting, processing or protecting the personal information of consumers. At the beginning of 2023, there was still no legislation offering data privacy rights to U.S. consumers, nor establishing privacy standards for companies on a national scale.

State legislatures have stepped into that gap and taken the lead on the issue. In 2022 lawmakers in at least 35 states considered legislation dealing with consumer data privacy, according to the National Conference of State Legislators.

The most common approach has been to propose comprehensive data privacy laws. Lawmakers in 25 states considered comprehensive measures last year. And that activity was actually the continuation of a trend of rapid growth in comprehensive state data privacy legislation since 2018, as documented by the International Association of Privacy Professionals.

But some states have taken a more piecemeal approach, considering measures targeted at specific areas of data privacy. For instance, last year 13 states took up bills dealing with biometric data privacy, nine considered measures addressing consumer genetic testing and six proposed children's data privacy legislation, much of it modeled after the sweeping measure enacted in California last year (AB 2273).

States Took Comprehensive and Piecemeal Approaches on Data Privacy in 2022



The flood of data privacy legislation has continued in 2023, with at least 25 states having introduced over 100 consumer data privacy measures as of mid-February. Comprehensive data privacy bills were introduced in all 25 of those states.

State Data Privacy Laws Pose Major Compliance Challenges for Businesses

The legislative momentum for data privacy laws at the state level is more than just a development to monitor, it is a reality to confront in 2023. This year new comprehensive data privacy laws go into effect in five states: California, Colorado, Connecticut, Utah and Virginia.

The California Privacy Rights Act and the Virginia Consumer Data Protection Act were implemented on January 1, the Colorado Privacy Act and the Connecticut Data Privacy Act will kick in on July 1, and the Utah Consumer Privacy Act becomes effective on December 31.

"Further regulations from the California Privacy Protection Agency regarding automated decision making, cybersecurity audits and privacy risk assessments remain outstanding," reported Law360®. "What is clear is that there will be no shortage of privacy compliance steps that organizations will have to take in 2023," the legal news service said.

These new laws impose several new compliance obligations for companies doing business in these five states. And while there are some common requirements, the incongruity in the details of these regulations is creating a costly "patchwork of state privacy laws," according to the International Association of Privacy Professionals.

The compliance challenges won't come solely from the comprehensive data privacy laws. As the State Net Capitol Journal reported, AB 2273, the California Age-Appropriate Design Code Act, signed into law by Gov. Gavin Newsom (D) in September 2022, "creates a litany of new requirements for California businesses operating online, not the least of which is a mandate to verify every visitor's age before allowing them access to a website."

The bill also requires business to complete a "Data Protection Impact Assessment" before offering new features or services on their websites to determine what risks the new features or services might pose to children and how those risks will be mitigated.

With several other states having taken up measures like AB 2273, businesses outside California could soon be subject to similar requirements.

Businesses have plenty of incentive to get compliance with such requirements right. According to Mike Swift, chief global digital risk correspondent for MLex®, an investigative news agency focused on regulatory risk around the world, the legal costs of data protection violations by U.S. businesses topped $2.5 billion last year, with "little to suggest that surge in regulatory risk and cost for companies is going to slack off at all in 2023."

Key takeaway: State lawmakers have taken the lead on data privacy legislation and are enacting sweeping new measures that are taking effect now. While the new laws share some important characteristics, they form a patchwork of assorted requirements in different jurisdictions. It is essential for company executives to stay apprised of the latest legislative developments and various compliance requirements.

Building a Multistate Data Privacy Compliance Program

Strategies for Developing a Multistate Privacy Compliance Program, available to Lexis+® subscribers, identifies six guiding principles for building a corporate compliance strategy that is nimble enough to deal with data privacy laws that vary from state-to-state and are evolving rapidly. Those six components are:

Transparency (Disclosure/Notice Requirements)

Every comprehensive state privacy law requires businesses to provide consumers with notice of their collection activities and disclose intended uses, data sales or any use for targeted advertising. Most of the new state laws only require businesses to include this information in their privacy policies, although California goes beyond this requirement to provide state residents with additional notices.

Consumer Rights

Privacy laws have historically provided consumers with certain rights in relation to their personal information. The five new state data privacy laws are no different. And while there is substantial overlap between the state laws, the precise contours vary in each state and require individual assessment.

Sensitive Data

Related to consumer rights more broadly are the specific rights that consumers have with regard to "sensitive" data. The categories of information that fall within this requirement can include personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition, sexual orientation, citizenship status, genetic or biometric information, personal data from a known child and precise geolocation information, depending on which state law is under consideration.

Consent

Consent plays an important role in all five state privacy laws going into effect in 2023 and is defined similarly as a clear, affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement. Laws in some of these states explicitly exclude "implicit" consent or a more general consent from meeting this standard.

Vendor Due Diligence

The new state data privacy laws have adopted the approach that in-house counsel will recall from the EU's General Data Protection Regulation (GDPR), which requires "controllers" of personal information to enter into data protection agreements with their vendors. The exact language varies a bit from state to state, but they share the common regulatory principles.

Data Security

State data privacy laws expand businesses' obligations regarding the notification of consumers when there is a data breach involving their personal information. The new laws include front-end data security requirements to protect against cyberattacks and are substantially similar across jurisdictions.

The information in this article is brought to you by LexisNexis® State Net®.
Please visit our web page to speak with a State Net representative and learn how the State Net regulatory tracking solution can help you monitor bills as they progress through committee as well as new laws that are enacted in each jurisdiction.

LexisNexis.com/**StateNet**
800-726-4566

State Net®

LexisNexis, State Net, Lexis+ and the Knowledge Burst logo are registered trademarks and State Net Capitol Journal is a trademark of RELX Inc. Law360 is a registered trademark of Portfolio Media, Inc. MLex is a registered trademark of MLex Limited. Other products or services may be trademarks or registered trademarks of their respective companies.
© 2023 LexisNexis. 4149092563 0323