



*Your AI & Data Privacy Expert*

PART 4 OF 6-PART SERIES

# STATE DATA PRIVACY LAWS



**THIS IS THE FOURTH OF A SIX-PART SERIES** of commentaries on data management, authored by Steve Britt, managing partner of Britt Law LLC. These commentaries review the new laws and regulations relating to data privacy and artificial intelligence.



Steve is a deeply experienced **corporate and technology attorney** with world-class cyber, data privacy & artificial intelligence expertise, including three international data certifications. He also has extensive experience with software licensing, cloud, SaaS and data hosting. He practiced law in Washington, D.C. and Virginia prior to establishing Britt Law in Charleston, South Carolina. Steve formed Britt Law to leverage his data management experience and to offer a wider range of legal services with flexible fee arrangements. This includes fractional general counsel and fractional data protection engagements.



## PART 4

### INTRODUCTION

More than 20 states have passed a comprehensive data privacy law while other data laws are being enacted regarding consumer protection, consumer health data, biometrics identification and the protection of youth from social media platforms. Regardless of how relevant data laws are defined, they will continue to be passed until all states (and Congress) have had their say on the collection and use of data.

The only issue that has been able to slow this tsunami has been the sudden arrival of generative AI. It is related to but differs from data privacy, adding a new set of rules for different data uses; i.e., the use of data by machines.

The new state data privacy laws vary significantly. Some do not apply to nonprofits while others do. Some apply to companies that collect records on at least 100,000 of their state residents while other states set the limit as high as 175,000 or as low as 35,000 residents. Two recent state laws (Nebraska and Texas) have no records threshold at all, so the collection of data on a single resident triggers the state's data privacy law.



There are other significant differences. For example, several states require that the business get affirmative consent from the consumer (i.e., opt-in) to the collection and processing of the user's sensitive information, while other states grant a right to opt-out of such processing. Some count biometric and geolocation data as personal information while others do not.

That said, state data privacy laws have a lot in common. For example, nearly all of them do the following:

- I. Define **“personal information”** as any information that identifies, relates to or could reasonably be linked to, directly or indirectly, a natural person, including device data and browser data such as shopping history and online preference data.
- II. Create a new category of data called **“sensitive information,”** which is information about a consumer's financial accounts, race, ethnic, genetic, religious, union membership, immigration, health or sex life.
- III. Grant broad data rights to users, including the right to know, access, correct, delete and either opt-in or opt-out of the processing of their personal information.
- IV. Require disclosure, before collection, of all categories of personal information collected by the business, the categories of third parties the data is shared with, the purpose of such sharing and how long that data will be retained by the third parties.
- V. Require that any third party that personal data is shared with execute a restrictive contract restricting its handling and use of that data.
- VI. Impose many other requirements, including rules for policies and procedures, recordkeeping, a right of appeal for the denial of data deletion requests and implementation of sound data security.

In most cases, these laws do not provide a private cause of action for violations of these laws, with the main exception being the Washington My Health My Data Act. But they also do not override or limit the application of civil tort (i.e., negligence) law and consumer protection laws, so they pose their own litigation risks.

## REGULATORY TRIGGERS

In order to avoid investigations, fines and penalties, companies need to take the following actions:

- I. **Update Privacy Notices:** The new privacy notices required under these laws are far different than what applied in the past. For example, California requires the use of CCPA's 12 statutory categories of personal information rather than treating it as a single class of data. All states require the disclosure of the “categories” of personal information collected, while only California actually lists categories. Since these notices are publicly posted, reviewing a privacy notice is the easiest action a regulator can take.
- II. **Honoring Opt-Out Rights:** There are several data subject rights that must be granted and honored. These include opt-in or opt-out rights for the collection of sensitive information, the sale of personal information and the use of personal information for targeted advertising and profiling. These are key enforcement triggers for regulators and violations of them are often cited in enforcement actions.

III. Data Protection Assessments: Almost all of the new data privacy laws require data protection assessments, weighing the benefits of data processing activities against the risks of such activities to users. These reports must also analyze the risk mitigation tools that have been adopted (i.e., encryption, deidentification, pseudonymization, data minimization, etc.) and must be available to regulators on request. They will surely become a favorite tool for regulators.

## KEY TAKEAWAYS

- The first step in complying with these laws is to conduct a comprehensive privacy impact assessment (i.e., data map). This is completely different from a review of data security compliance, which focuses on access controls, least privilege, remote desk protocol, MFA, etc.
- A privacy impact assessment analyzes the personal information collected, how it is collected, from whom, in what jurisdiction and who it is shared with for what purpose.
- This granular analysis must be conducted by every office that handles personal information. A special privacy committee should be formed to ensure that the data practices of the entire enterprise are reviewed in the context of the special terms in these statutes.
- The assessment should include a review of the company's ability to tag, track and recover individual stakeholder records and should review relevant policies and procedures, employee privacy training and the processing of data subject requests.
- A data map can take several months, but it will educate senior management across the company on what these laws are all about, what they require and where the company may be falling short. Its outputs will map directly into a data privacy program.
- If AI is already a component of your business or is being contemplated, the assessment can incorporate AI regulatory principles, which will greatly assist the planning and preparation for future laws and regulations.
- Done correctly, a privacy and AI impact assessment will pave the way for a sound and comprehensive data management program. Once implemented, management of this program will be relatively straightforward as inevitable changes in laws and regulations occur.

**To learn more, contact Steve Britt at [steve@brittlawllc.com](mailto:steve@brittlawllc.com).**