



Your AI & Data Privacy Expert

PART 1 OF 6-PART SERIES

DATA MANAGEMENT: *What Now, What Next & What to Do*



THIS IS THE FIRST 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 1

SERIES INTRODUCTION

Data breaches and ransomware attacks continue to wreak havoc on U.S. businesses, directly impacting the availability and cost of cyber insurance.

Just under the surface of all this turmoil is an evolving wave of data privacy and artificial intelligence laws that will greatly alter the management of all forms of data, not just the “personal information” regulated under data privacy laws.

We have pretty good clarity about the structure of state data privacy laws, but it seems that each new law and each new set of regulations promulgated under these laws are expanding in ways we could not have envisioned a year ago. So, nothing is really settled.

The federal government, on the other hand, is still trying to reach a consensus on a federal data privacy law to bring some semblance of uniformity to this landscape, but those prospects remain dim. Meanwhile, artificial intelligence has captured everyone’s attention, including Congress’, frustrating any consensus on data issues.

Meanwhile, Europe has enacted the “first in the world” artificial intelligence act that will do for artificial intelligence what General Data Protection Regulation (GDPR) did for data privacy – take the lead worldwide on a ground-breaking regime. Just as GDPR automatically applied to U.S. companies collecting personal data on European Union (EU) residents, the EU AI Act will automatically apply to U.S. companies releasing artificial intelligence (AI) tools, systems and technologies into the European market from any location.

With the introduction of generative AI, states are moving ahead with new artificial intelligence laws and regulations. AI terms are sometimes grafted onto state data privacy laws or regulations but are just as likely to be enacted as separate statutes. It is impossible to predict how this will all play out over time as the Federal government certainly intends to legislate on AI as well.

But that does not mean clients should not make wise use of this time. There are several strategic actions they can—and should—take now to begin orienting their organization toward sound data management principles.

Our goal in this series is to help companies understand what is happening, where it is all going and what they should do now to prepare. It is a tricky line to walk. We don't want to drown our readers in legalese, and as much as has happened in the past two years, much is yet to happen.

For example, over 20 new state data privacy laws have passed and 19 will have gone into effect by the end of 2025. Of those in effect, only a few states have issued regulations. But those regulations are extremely complicated and certainly demand attention. Meanwhile, we have four new state artificial intelligence laws in effect, with broad AI risk assessment regulations on the way.

So, as the waves of data privacy laws continue to roll in, AI is building enormous strength right behind them. It is wise to begin the process of building a sound data privacy program for several reasons. For example:

- I. First, data privacy poses a substantial data configuration challenge. A company must be able to tag, track, recover and delete individual stakeholder records from its on-prem and cloud servers as well as from its offline storage. Under a new California law (AB 1008), those obligations may apply to personal information contained within AI-system models if that data is capable of being accessed or output.
- II. Second, the analysis of data issues begins with an assessment of the types of personal information collected by a business, how it is collected, from whom, in what jurisdictions and to whom that data is shared with for what purpose. The language of data privacy will be new to your CIO or CISO, who have had their hands full interpreting the rules on data security.
- III. Finally, operationalizing data subject requests, opt-in and opt-out rights, data protection agreements (or BAAs), audits, employee training, user verification and other compliance actions are simply too complex to attempt on short notice or without the requisite expertise.

Artificial intelligence brings its own governance challenges, and companies must be careful about incorporating this technology into their operations without an accurate understanding of the compliance issues that come with it. Sound AI governance principles must be put in place in the earliest planning stages of artificial intelligence and must operate throughout the lifecycle of the system.



TOPICS IN THIS SERIES

This series covers the following issues in separate commentaries. Each one will summarize the new developments in these areas and translate them into key takeaways:

PART 1: Series Introduction

PART 5: HIPAA Tracking Technologies

PART 2: EU Artificial Intelligence Act

PART 6: Series Conclusion

PART 3: State Artificial Intelligence Laws

PART 4: State Data Privacy Laws

A WORD ABOUT DATA BREACH STATUTES

A quick comment about data breach notification statutes, which exist in every state. Although outside the scope of this series, it is worth noting that at least twelve of the 50 state data breach notification laws authorize a private cause of action for violations of the statutes. Also, the definitions of “personally identifying information” under these statutes are constantly expanding and often now include biometric data, GPS location data, profiling data and the social media data of youth. This continually expands the risks of data breaches.

Also, data breach and data privacy have effectively merged into the larger concept of data protection. Regulators are now using data breach notifications as a trigger for auditing the victim’s data protection compliance. So companies should get their data protection house in order as soon as they can.

KEY TAKEAWAYS

- Seven years after the enactment of GDPR, the adoption of data privacy in the U.S. has taken its own unique path. Congress has been unable to agree on a comprehensive Federal statute, so the states have proceeded on their own.
- California was the first state to do so in 2020 and has dominated the U.S. data privacy discussion ever since. But that is changing with 20+ new state data privacy laws and Colorado is certainly making its presence felt in this area.
- Several states and Federal agencies are now regulating a whole new category of personal information called “consumer health data,” which is any information about a consumer’s past, present or future physical or mental health. Don’t mistake this for Protected Health Data (PHI) under HIPAA. That data is expressly excluded. These laws and regulations are greatly expanding the regulatory attack surface.
- Virtually all of the new state laws require data protection assessments that must be made available to regulators upon request, giving regulators an easy tool for auditing a company’s compliance status.
- In California, broad regulations relating to cyber audits, data risk assessments and automated decision-making technologies (ADMT) are on the way and will accelerate action on all of the issues discussed in this series.

To learn more, contact Steve Britt at steve@brittlawllc.com.