BRITT LAW

J. STEPHEN BRITT, ESQ.
Managing Partner
steve@brittlawllc.com
(703) 989-7525
BRITTLAWLLC.COM

OCTOBER 2025

EXPERT GUIDE TO AI & DATA PRIVACY

I. Introduction

The legal requirements for data privacy & artificial intelligence ("***AI***") (collectively, "***data management***") are complex, confusing and rapidly evolving. Many new laws & regulations are on their way, so nothing is settled. That said, many legal terms and approaches are sufficiently clear that companies can reliably prepare for and implement a data management program that will shield them from regulatory actions and litigation.

This guide is a high-level review of relevant issues & considerations. It seeks to demystify the evolving legal regimes so companies can manage all these new risks.

II. Your Expert

Steve Britt is an expert in data privacy & artificial intelligence law. He holds the **AIGP** (Artificial Intelligence Governance Professional), **CIPP/E** (Europe for GDPR) and **CIPM** (Privacy Manager) certifications from the IAPP (www.iapp.org).

Steve also serves as General Counsel of the **National Artificial Intelligence Association** (www.thenaia.org), the national trade association for AI.

III. The Current Legal Landscape

In the past few years, GDPR, the EU AI Act, 23 state data privacy laws, consumer health data and state AI laws have been enacted. Social media and youth protection laws are imposing new rules for parental consent & age verification and global privacy controls are being mandated.

While State data privacy laws do not authorize a private right of action, class actions are being filed under state and Federal wiretapping laws and regulators are levying large fines and procuring large settlements. We are still in the early innings, but with AI already here, companies need to act now to implement defensive measures.

IV. How Does Data Privacy Relate to AI?

AI does not supersede data privacy. While both terms relate to data, they are distinctly different legal regimes. If personal information is processed by AI, compliance with both sets of laws is required.

Data privacy regulates the collection and use of "***personal information,***" which is any information – **any information** – that can identify a natural person. It includes IP addresses, cookies, device data, browser data and online search history. Users are granted broad data rights (i.e.; the right to know, access, correct, delete and opt-out of data transfers) that must be properly processed. They require detailed privacy notices, reasonable data security and detailed data protection assessments that must be available to regulators on request.

AI laws govern the automated processing of any type of data, not just personal information. Uploading *personal information* into an AI model triggers both laws. The legal requirements for AI technology are extensive, including detailed risk assessments under trustworthy standards. **And unlike data privacy laws there is no shield from private lawsuits**.

V. What is Responsible AI Development?

NIST defines the principles of responsible AI development. There are no clearly established metrics for these standards. That does not mean you don't have to worry about them. That means you must develop and deploy AI technology in accordance with these principles and be able to demonstrate you reasonably meet them:

- **Valid & Reliable:** System trained on valid data and performs as intended;
- **Accurate & Robust:** System produces true results & maintains performance levels,
- **Safe:** System does not endanger life, health, property or the environment,
- **Secure & Resilient:** System is secure & can return to normal after intervention,
- **Accountable & Transparent:** Consequences of use traceable to responsible parties,
- **Explainable & Interpretable:** Algorithms, processes & operations are fully explained,
- **Privacy-Enhanced:** System safeguards human autonomy, identity & dignity, and
- **Fair with Harmful Bias Managed:** System promotes equality, fairness, justice & personal freedom

VI. Compliance is All About Assessments

Both data privacy & AI laws rely heavily on assessments with specific rules on what they must contain and how they must explain data processing. These will become critical regulator tools for determining the quality and scope of your program compliance.

AI laws require assessments of AI technologies that are deemed "***high risk***" (EU) or that make "***consequential***" (Colorado) or "***significant***" (California) decisions about consumers. These terms all mean decisions affecting access to or the terms of these pursuits:

- Educational opportunities
- Employment, jobs or contracts
- Banking, loans or financial services

- Government benefits or services
- Healthcare services
- Housing
- Insurance
- Legal services, voting or access to justice

Data privacy laws require assessments for processing activities that pose a ***significant risk*** to consumers. Those are the risks resulting from (i) the sale of personal information, (ii) the processing of sensitive data, (iii) the transfer of data for targeted advertising, (iv) the use of data for profiling, and (v) the use of personal information to train automated decisionmaking technologies ("***ADMT"***).

Here is an overview of these new assessments:

(a) State Data Protection Assessments. Every company that poses a significant risk to consumer privacy must prepare an assessment that weighs the benefits of each data processing activity against the risks of such processing, taking into account any safeguards that mitigate such risks. Those reports must be available to regulators on request.

(b) AI Risk Assessments. AI risk assessments must describe all foreseeable harmful uses of the system, data provenance, the logic of the algorithms, protections from algorithmic discrimination and how the system works. The EU requires compliance assessments before any AI Systems can be released into Europe and registration in an EU database.

(c) CPPA Cyber Audits, Risk Assessments & ADMT Regulation: In September 2025, the California Privacy Protection Agency ("***CPPA***") released broad new CCPA regulations. Once finalized, they will require detailed and independently prepared annual cyber audits. They will also require (i) broad risk assessments, and (ii) a right of access to ADMT, a right to opt-out of its use and the right to appeal ADMT decisions to human reviewers. Companies need to plan for these new requirements. California's ADMT requirements will spread to other states since new state data privacy laws already regulate the automatic processing of data.

VII. Data Security Standards & Confidential Computing

All data privacy laws require protection of the data from hacking, loss and unauthorized use. These standards are often stated generally, such as the requirement for "***reasonable data security***." Or they require the implementation of "***administrative, technical & operational measures"*** sufficient to protect the ***"confidentiality, integrity & availability***" of data.

EU's Digital Operations Resilience Act ("***DORA***") is more specific by requiring protection of data "***in use***." That term is also found in Colorado's AI Act. California's new ADMT regulations describe the "***use of privacy enhancing technologies ("PETs") such as trusted execution environments, federated learning, homomorphic encryption and differential privacy***" as safeguards to be reported in risk assessments. The term trusted execution environment ("***TEE***") is generally associated with Confidential Computing.

Confidential Computing protects data actively ***in use*** in the processor and memory. A TEE is a hardware-enforced, cryptographically-attested location where sensitive data can be decrypted, viewed and processed only by authorized users. This technology is seeing rapid adoption for financial services, healthcare, government and other highly sensitive processing. It is offered with LLMs in major data centers and can be deployed in edge applications. It greatly enhances protection of AI models and its reference in the new CPPA regulations will spread its adoption to other state regulators.

VIII. Regulatory / Litigation Risk Triggers

Our data management advice always focuses on these triggers for fines & penalties:

- Improper privacy notices (content, location & processing),
- Failure to honor data subject rights, including right of opt-out of sensitive data,
- Improper use of tracking technologies (cookies, pixels & web beacons),
- Inadequate data security (confidentiality / integrity / availability of data),
- Improper use of copyrighted content,
- Failure to validate, secure, disclose use of and monitor AI,
- Improper or failure to provide consumer health data notices,
- Failure to prepare cyber audits & risk assessments, and
- Improper design of third-party consent tools

IX. Compliance Game Plan

Companies should design and implement a comprehensive data management program that is tuned to their specific operations. If they are using AI, they should institute AI governance, analyze their operational risks, perform assessments, determine consequential decisionmaking, implement strong data security controls (including confidential computing for highly sensitive operations) and continuously monitor & test all components.

X. How We Can Help

We help companies navigate these risks. We operate on a **fixed fee** or **hourly** basis, a **consulting rate** or as **fractional data counsel**. We will help assess your actual data practices and incorporate all compliance requirements into your product roadmap. The goal is not perfection, but rather, a comprehensive good faith effort at compliance.

STEVE BRITT
Britt Law LLC
Managing Partner
Phone: 703-989-7525
Email: steve@brittlawllc.com
Web: brittlawllc.com