Managing Data Security and Privacy Risks in Enterprise AI

Mar 04, 2025

Categories:

Publications

Authors:

Barbara Bennett
Mason C. Clutter
Matthew R. Schantz

Artificial intelligence (AI), particularly generative AI, thrives on vast amounts of data, fueling AI capabilities, insights, and predictions. But with this reliance on data comes potential privacy and security risks. And because AI tools are data-rich by nature, they're a potential gold mine for cyber criminals prowling for sensitive or proprietary data to exploit.

The latest AI tools have acted as an accelerant, testing the limits of existing laws while raising novel legal questions for courts to adjudicate with little precedent to lean on. Who "owns" the troves of data that are fed into generative AI (GenAI) systems, and what safeguards may attach to its use? Who owns the output, and how might output impact individuals? And, not least, who's responsible for ensuring that AI tools are being developed and used in a responsible and lawful manner—with appropriate data security and privacy safeguards?

This article covers potential data security and privacy risks associated with AI[1], applicable laws and regulations[2], and what companies can do to accomplish their goals in a privacy-respecting manner[3], while promoting cyber resilience as we both embrace and brace ourselves for ever-more-sophisticated AI tools.

Balancing Risk and Reward with AI

While enterprise AI presents opportunities to achieve business goals in a way not previously conceived, one should also understand and mitigate potential risks associated with its development and use. Even AI tools designed with the most robust security protocols may still present a multitude of risks. These risks include intellectual property theft, privacy concerns when training data and/or output data may contain personally identifiable information (PII) or protected health information (PHI), and security vulnerabilities stemming from data breaches and data tampering.

Courts are now fielding an uptick in lawsuits related to unintended and illegal biases in AI outputs and automated AI decision-making and profiling, ranging from employment discrimination and defamation claims to health care access and insurance coverage claims. AI has also been at the center of investigations and enforcement actions undertaken by federal agencies like the Department of Labor and Federal Trade Commission (FTC). For example, the FTC filed a complaint

against Rite Aid alleging its use of facial recognition software resulted in misidentifying customers as shoplifters and that the company failed to train its employees on how to appropriately use the system, including how to anticipate and address false positives—many false positives, in fact.

Compounding the legal risks are the potential reputational risks companies may face when an unintended mistake or violation originating with an AI tool comes to light. Examples include lack of human oversight and decision-making, the disclosure of private, confidential, or proprietary information, or unintended biases or other harms. Accordingly, the development and deployment of AI technologies should include a robust AI governance program in which privacy and data security considerations are entrenched at every level.

Data Security and Privacy Regulations Applicable to AI

Privacy and data security in the context of AI are interdependent disciplines that often require simultaneous consideration *and* action. To begin with, advanced enterprise AI tools are trained on prodigious amounts of data processed using algorithms that should be—but are not always—designed to comply with privacy and security laws and regulations. Those laws, primarily at the state level, are still evolving and can vary considerably from one jurisdiction to the next. Another concern is whether legal requirements, like consent or copyright, may attach to the underlying training data. Business deals and contracts can likewise be implicated. For example, a company could face lawsuits and penalties if its use of AI is found to breach contractual obligations.

In the United States, unlike other countries, Congress has yet to enact a comprehensive national privacy law; the same is true for private-sector development and use of AI. States are now beginning to fill that gap. Currently, 19 states have enacted comprehensive privacy laws, and four states have what we would call "generally applicable" laws addressing AI applications in the private sector (i.e., non-sectoral-specific or government-only laws). The Colorado Artificial Intelligence Act, for instance, imposes risk management and disclosure obligations on companies that develop or deploy "high-risk AI systems," typically those involved in providing or denying consumers access related to healthcare, education, employment, housing, government and financial services.

California is another state at the forefront of regulating AI, as with privacy. In 2024, California passed a several AI laws, including Assembly Bill 2013—Artificial Intelligence Training Data Transparency—requiring developers of covered GenAI

systems to disclose information about the nature and source of the data on which their AI systems are trained. California also passed the California AI Transparency Act. Effective January 1, 2026, this law will require covered providers of GenAI tools to roll out AI detection tools and "watermarking" features that indicate whether audio, image, or video content is AI-generated.

It's clear that AI will be a focal point at the federal level, too. Included in the Trump administration's first week of executive orders was one revoking President Biden's Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, along with another order from the new administration titled Removing Barriers to American Leadership in Artificial Intelligence. This order directs the creation of an action plan to achieve the Trump administration's AI strategy and policy goals. So, we will need to wait and see what is included in that plan and whether and how it may impact private-sector development and use of AI in the future.

In the meantime, let us not forget the applicability of the various state privacy and security laws to AI generally. A law need not be specific to AI to apply to development and deployment of an AI system, which calls into play the patchwork of existing and future state-level governance frameworks.

These are just a few examples of what we expect to see in a very busy legislative year across the country. AI's potential to exacerbate data security and privacy risks for both individuals and organizations, as well as the need to adopt rigorous data provenance and governance practices, are common themes ripe for legislation and are, therefore, the underpinnings of best practices for the development and use of AI.

Promoting Cyber Resilience in the Era of AI

As it pertains to data security, key cybersecurity measures include:

- Implementing multi-factor authentication and strict access controls.
- Maintaining patch discipline and segmented network architecture.
- Utilizing data anonymization and pseudonymization techniques.
- Implementing data masking to protect sensitive information.
- Deploying continuous monitoring tools to detect anomalies and latent threats.
- Training AI models to withstand adversarial inputs.

Privacy and Security in Governance Frameworks

Emerging laws and regulations related to AI are thematically consistent in their emphasis on accountability, fairness, transparency, accuracy, privacy, and security. These principles can serve as guideposts when developing AI governance action plans that can make your organization more resilient as advances in AI technology continue to outpace the law.

Good AI governance combines different risk-management frameworks to address an organization's legal requirements and values while establishing appropriate practices to safeguard privacy and protect their information assets, employees, and customers. Importantly, AI governance should be undertaken in partnership with a company's data governance, security, and privacy programs.

Developing an AI governance program typically starts with mapping how AI technology is being used (and by whom), identifying and quantifying risks, and implementing controls to effectively manage those risks. This process can help companies not only stay compliant as they innovate with AI but also defend against litigation and enforcement actions.

Best Practices for Organizations

Below are a few best practices that can be incorporated into strong enterprise AI governance frameworks to mitigate data security and privacy risks while benefiting from AI's opportunities:

- Establishing clear data provenance and governance practices.
- Designating cross-functional AI leads within the organization (legal, IT, HR, etc.).
- Providing employee-level training on AI tools and acceptable uses.
- Updating licensing agreements to reflect new transparency requirements.
- Maintaining awareness of evolving federal and state-level regulations.

Frost Brown Todd has a dedicated team that advises clients on their unique enterprise-wide AI integrations, helping them institute governance programs, proactively address data security and privacy concerns, and navigate a host of other AI opportunities and mitigate potential risks in their industry. To learn more about how Frost Brown Todd can help empower your company's AI journey, contact the authors of this article or any attorney with the firm's Artificial Intelligence team.

Frost Brown Todd ATTORNEYS

Lexology Masterclass Series

This article was adapted from a webinar presented by Frost Brown Todd in partnership with Lexology's Masterclass programming. All three webinars in this series can be streamed for free by clicking on the links below.

- **Webinar: AI in the Workplace**
- **Webinar: AI in Products/Services Contracting**
- **Webinar: AI in Data Security & Privacy**

Learn More