CEP Magazine - February 2024

John Brushwood (john.brushwood@traliant.com) is Compliance Counsel at Traliant in Arlington, Virginia, USA. He specializes in data privacy and cybersecurity law.

Navigating the intersection of data privacy laws and the rise of AI

By John Brushwood, JD, CIPP

Artificial intelligence (AI) has seen significant advancement and adoption over the past few decades. 2023 alone was a defining year for AI with the emergence of a sophisticated generative AI tool, ChatGPT, which has made AI more easily accessible to the public, speaking particularly to those with low or no coding experience.[1] As a large, language model-based chatbot that can compose written content or engage in human-like conversational dialogue, the intention of ChatGPT is to enhance productivity and efficiency. More broadly, AI is being implemented across most businesses today to streamline processes and understand data trends, with many leaders feeling that AI will substantially transform their industry and shape the future of work.[2]

AI presents opportunity and risk

While AI brings significant time and cost savings to businesses and employees, the degree to which these technologies have evolved brings significant risk and can be detrimental if not governed properly. Data privacy is one area where risk can be at its highest. For instance, AI tools used for automated decision-making may violate not only data privacy laws but also sector-specific laws—such as the Fair Credit Reporting Act, Equal Credit Opportunity Act in banking, and Title VII of the Civil Rights Act in the context of hiring and promotions. Additionally, many AI tools do not comply with current data privacy rules, such as those included under Europe's General Data Protection Regulation.[3] Lastly, businesses also run the risk of employees improperly disclosing personal or business data into tools like ChatGPT.

As AI continues to catch the eyes of business leaders looking to enhance processes, it's also top of mind for policymakers as well. At the federal level, the Biden administration implemented the AI Bill of Rights in 2022,[4] followed by an Executive Order in 2023,[5] both provide guidance on how to ensure AI is safe, secure, and trustworthy. There's also been action at the state level: California proposed the requirement of data impact assessments for automated decision-making,[6] and Connecticut enacted a bill that regulates how AI is used for personal data privacy.[7]

While these laws directly regulate the intersection of data privacy and AI, the reality is that many organizations are unprepared to comply with them. Further, taking a reactive approach to AI regulation is no longer a feasible or safe option, putting compliance leaders in a position today where they must create a proactive AI governance strategy that avoids the risk of unlawful conduct and the penalties that follow. While it may seem like a daunting task with so many existing and proposed laws currently in flux, there are essential steps they can take today that can significantly reduce data privacy concerns.

Establish an AI governance committee

Determining who will lead AI governance at an organization is the first step to ensuring it's properly managed and enforced. There is no one-size-fits-all approach to an AI governance committee; depending on the organization's size and structure, it can comprise individuals across teams, such as privacy, legal, IT, and more.

Once a committee is established, a comprehensive AI governance framework must be created. This framework outlines rules, procedures, and safeguards that the organization is implementing for the ethical—and lawful—use of AI. This framework will also be strictly enforced and trained across the entire organization.

There are many examples of voluntary frameworks available today, such as the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF), which may be used as a guide or copied entirely.[8] Tennessee's privacy law, House Bill 1181 Section 47-18-3213, provides an affirmative defense for organizations that voluntarily use NIST's RMF, meaning that organizations that proactively elect to implement voluntary governance frameworks like the RMF into their policies may avoid penalties from AI laws that will be enacted in the future.[9]

This AI governance framework is also where policies should be created around the use of specific AI tools like ChatGPT. Establishing what is and is not permitted when it comes to using AI tools allows businesses to comply with data privacy laws and uphold the ethical standards of their organizations. One example of this could be preventing a lawyer from asking to use ChatGPT to write a legal pleading. Even if the attorney does not input any personal data that violates data privacy laws, using ChatGPT to write a legal pleading would violate several laws and ethical obligations.

Lastly, the AI governance framework should also include reporting and incident response protocols, which will likely vary based on the size and structure of the organization. For instance, large international corporations will sometimes have separate privacy, security, IT, and legal teams, with the privacy team as the first point of contact for any employee who initially discovers an incident. Rapid incident response is also important for minimizing harm and risk. Many data breach laws establish a 72-hour reporting requirement that, if met, will reduce or even eliminate penalties. Alongside these procedures, organizations should train their employees on how to spot an incident and which team they should report it to.

Update data privacy training programs

Data privacy should be a cornerstone of employee training—when they start working for the company and on a continuous cadence during their tenure as new laws and regulations emerge. It is essential to update training programs to ensure employees are trained in data privacy laws and their intersection with AI governance standards.

Employees should be trained regularly on AI governance framework in its entirety so they're both aware of and familiar with evolving laws and regulations. This includes understanding the established permissions around tools like ChatGPT and, if needed, how to report incidents quickly and thoroughly to reduce harm to affected persons, reduce fines by regulators, and decrease reputational harm to the organization. Amplifying the knowledge base around a rapidly evolving technology such as AI is the best way to mitigate its potential risks but also enable its safe and lawful use in instances where it can benefit the company.

Designating AI champions among employees is also a good way to safely adopt AI tools and ensure the applications are safe. AI champions can advocate for the use cases that benefit the organization but also be keen on how they could be misused. Instilling this type of culture around technology creates an organizational approach, putting the onus of safe AI use on everyone—not just managers and leaders.

Keep apprised of evolving laws and regulations

The intersection of data privacy and AI is constantly evolving, especially as new and innovative technologies disrupt the status quo. To accurately monitor data privacy and AI intersection, organizations must monitor legislation in both sectors to understand the big picture.

For AI-specific legislation, the National Conference of State Legislatures covers key legislation related to AI issues generally.[10] The Brennan Center for Justice's Artificial Intelligence Legislation Tracker[11] and the International Association of Privacy Professionals' (IAPP) Global AI Legislation Tracker[12] also serve as useful resources to identify legislative policy and developments.

To accurately monitor data privacy legislation, valuable resources are the IAPP's state,[13] federal,[14] and global data privacy trackers.[15] For companies with a national or global presence, it's even more critical to keep an accurate pulse on all laws and regulations, as many can vary across regions and apply to different employees. There are 11 states with comprehensive data privacy laws in place, yet all vary to some degree.[16] For example, California's Consumer Privacy Act goes further than other states and even national-level comprehensive data privacy laws regarding the use of anonymous data. Under the law, if an organization deidentifies data so that it may not be traced back to an individual, it must *also* ensure that no one can reidentify that data. This is particularly meaningful when it comes to AI tools because they are capable of reidentifying an individual with very little data.

Additionally, proposed bills in Massachusetts, New Jersey, Pennsylvania, North Carolina, and several other states have similar rights in preexisting privacy legislation but differ in implementation and enforcement. The U.S. privacy law landscape is a patchwork of state and federal laws without a single comprehensive regulation. The bottom line is that data privacy concerns are more vital than ever as AI tools continue to evolve rapidly; however, if organizations proactively monitor developments within data privacy and AI laws, they may head off problems before they arise.

We're certainly living in progressive times where advancements in digital tools are rapidly transforming industries and the way we work. Yet, ensuring AI governance frameworks evolve alongside them is equally crucial. Organizations can be proactive with AI by establishing an AI governance committee to guide the adoption of a comprehensive framework, training employees and AI champions on the importance of this framework, and making sure that everyone in the organization is knowledgeable about legislative and regulatory evolutions. This type of proactive approach to governing data privacy and AI minimizes the risk of monetary penalties, reputational harm, and litigation while creating a safe and ethical workplace.

Takeaways

- The evolving sophistication of artificial intelligence (AI) can bring business benefits but also risks when it comes to data privacy laws.
- Businesses need to take a proactive approach to emerging laws and regulations around AI use.
- Establishing an AI governance committee is essential to creating a comprehensive AI governance framework.
- Updating employee training programs to include acceptable use policies for AI tools will help businesses mitigate risk.

- Laws and regulations are constantly evolving—and vary state to state and country to country—making it important for business leaders to stay updated on what policies affect their business.

[1] McKinsey, "The state of AI in 2023: Generative AI's breakout year," August 1, 2023, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year.
[2] Mike Bechtel, "The future of AI: Seeing the forest for the trees, and the forests beyond," Deloitte, accessed December 11, 2023, https://www2.deloitte.com/us/en/pages/consulting/articles/the-future-of-ai.html.
[3] Daily Dashboard, "CNIL orders Clearview AI to stop processing images," IAPP, December 16, 2021, https://iapp.org/news/a/cnil-orders-clearview-ai-to-stop-processing-images/.
[4] The White House, Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People," October 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[5] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
[6] A.B. 331 2023-2024, Reg. Sess. (Cal. 2023), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB331.
[7] Jordan Crenshaw and Michael Richards, "Connecticut: Introduction of new AI regulations in State Government," *DataGuidance*, August 2023, https://www.dataguidance.com/opinion/connecticut-introduction-new-ai-regulations-state.
[8] National Institute of Standards and Technology, "NIST Risk Management Framework," updated November 8, 2023, https://csrc.nist.gov/projects/risk-management/about-rmf.
[9] Public Chapter No. 408 §§ 47-18-3201(18) (Tenn. 2023), https://www.capitol.tn.gov/Bills/113/Bill/HB1181.pdf.
[10] National Conference of State Legislatures, "Artificial Intelligence 2023 Legislation," updated September 27, 2023, https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation.
[11] Brennan Center for Justice, "Artificial Intelligence Legislation Tracker," August 7, 2023, https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-legislation-tracker.
[12] IAPP Research and Insights, "Global AI Legislation Tracker," IAPP, August 2023, https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf.
[13] Andrew Folks, "US State Privacy Legislation Tracker," IAPP, last updated December 8, 2023, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[14] Müge Fazlioglu, "US Federal Privacy Legislation Tracker," IAPP, last updated September 2023, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/.
[15] IAPP, "Global AI Legislation Tracker," September 2023, https://iapp.org/resources/article/global-ai-legislation-tracker/.
[16] Bloomberg Law, "Which States Have Consumer Data Privacy Laws?" last updated on November 27, 2023, https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/.