# Navigating data challenges and compliance in AI initiatives

**By Anup Iyer, Esq., Moore & Van Allen**

**JANUARY 19, 2024**

Data serves as the foundational element for artificial intelligence (AI) models, enabling algorithms to discern patterns, forecast outcomes, and provide insights. The advent of generative AI, which relies extensively on vast and varied data sets to create new content, underscores the importance of data in this context.

While AI initiatives such as generative AI present novel opportunities, they also introduce complex legal challenges related to data privacy, intellectual property rights, ethical considerations, and contractual obligations. This article looks at some of these legal challenges and provides guidance for in-house counsel on establishing frameworks for responsible utilization of data in AI initiatives.

## Data privacy regulations

In today's digital world, the European Union's General Data Protection Regulation (GDPR) and the U.S.'s California Consumer Privacy Act (CCPA) are key laws that deal with data privacy. GDPR has been around since May 2018 and focuses on safeguarding the personal data of EU residents by setting rules on how organizations handle this data. CCPA, in effect since January 2020, boosts privacy rights and consumer protection for California residents.

Given the importance of these legal frameworks, following data privacy laws isn't just about meeting regulations; it is a key part of responsible data management. Organizations can strengthen their compliance by implementing several measures.

Regular data audits can show how data is being collected and stored, highlighting areas for improvement. By integrating privacy-by-design principles in AI initiatives, whether developed in-house or acquired through third party vendors, organizations can focus on the importance of data privacy at the outset and lower the risk of data exposure. Transparent and easily accessible privacy policies can clarify the organization's stance on data use, storage, and protection.

For collecting personal data, organizations can establish options for obtaining explicit, informed consent from data subjects. Organizations can appoint Data Protection Officers who can serve as a centralized resource for compliance monitoring and managing stakeholder communication. These compliance efforts can be made more robust by offering ongoing staff training and expert legal advice.

By investing in training and legal advice, organizations can not only comply with current laws but also prepare for evolving legal environments. This way, they transform compliance from a mere legal requirement into a key component of ethical conduct and risk management.

## Intellectual property issues

IP laws add another layer of complexity to the already complicated world of AI data collection. Issues about who owns the data often become more urgent. For example, who has the rights to data collected from various places like user-created content or data from third-party sources?

*While AI initiatives such as generative AI present novel opportunities, they also introduce complex legal challenges related to data privacy, intellectual property rights, ethical considerations, and contractual obligations.*

Also, the increase in AI-created data — data made by AI algorithms and not people — makes things more complicated. Who owns this data: the people who made the AI model, the users, or maybe even the AI model itself? These questions often don't have easy answers because both technology and legal rules are always changing. The lack of clear laws or settled court cases in this area makes it even more important for organizations to be proactive.

Organizations can preemptively tackle these issues by using legal tools like data licensing agreements and contracts that clearly state who owns the data. These documents can outline not just ownership but also the scope of usage rights, limitations, and responsibilities for all parties involved. By proactively defining these parameters, organizations can reduce legal confusion and fortify the base for their AI initiatives. Adopting such a proactive legal strategy not only reduces potential risks but also helps with accelerated commercialization and broader adoption of AI technologies.

## Consent and ethics

Collecting data from individuals frequently requires informed consent, which must be obtained through transparent methods that clearly outline the scope and purpose of the data usage. This

informed consent is not merely a legal formality but a fundamental ethical obligation. It builds trust between individuals providing the data and the organization collecting it, giving the individual some control over their own information.

*IP laws add another layer of complexity to the already complicated world of AI data collection. Issues about who owns the data often become more urgent.*

Ethical concerns are important not just during data collection but also when the AI system is in use. Biased data can lead to biased algorithms, which can result in unfair or discriminatory outcomes. Making sure AI is fair isn't an optional extra; it's increasingly becoming both an ethical and legal requirement. To mitigate these issues, organizations can implement various measures through multiple stages of the AI initiative. This comprehensive approach can involve initial data audits to check for existing bias, rectification methods such as re-sampling to balance data sets, and the use of fairness-aware algorithms.

Additional checks could involve outside audits and ethics boards made up of experts from different fields to oversee AI initiative development and deployment. By putting all these pieces together into one framework, organizations can do a better job of fighting bias and meeting the ethical and legal standards needed for AI initiatives.

## Contractual obligations

In the complicated world of collecting and using AI data, organizations should see contracts like data licensing agreements, non-disclosure agreements (NDAs), and service agreements as key tools for lowering risk. For instance, to reduce ambiguities that may lead to legal disputes, organizations can use data licensing agreements. These agreements are key for clearly defining the scope of data usage, ownership rights, and compliance obligations.

Additionally, organizations should use non-disclosure agreements to protect proprietary or sensitive information exposed during the data collection or analytics process. This is particularly important when engaging with third-party data providers or analytics services, as these agreements often include confidentiality obligations and outline the legal consequences of unauthorized disclosures.

Lastly, organizations can establish service agreements to set operational and quality standards for services related to data collection, storage, or analytics. Putting these agreements in place sets clear standards and ways to hold people accountable, providing organizations with legal recourse if these standards aren't met.

## Role of in-house counsel

In today's world of data-focused AI initiatives, one of the main jobs for in-house lawyers is to establish and keep up-to-date policies about how data is collected, stored, and used in AI initiatives. These policies must be continuously updated to keep up with new laws, ethical guidelines, and changes in technology and business practices. In-house counsel should work with various departments, including the technology, human resources, and marketing teams, to ensure that these policies are consistently applied across the organization.

Another critical responsibility of in-house counsel is to educate and train employees on data governance best practices and legal compliance. They can run regular training sessions, develop educational materials, and communicate important legal updates to keep staff informed and equipped to manage data responsibly.

In-house counsel can also take the lead in drafting, reviewing, and negotiating contracts that pertain to AI initiatives and data, such as data licensing agreements, non-disclosure agreements, and service agreements. This role requires a deep understanding of the organization's objectives, potential legal risks, and current contractual norms in the industry. By meticulously structuring these agreements, in-house counsel can reduce ambiguities and protect the organization from unnecessary legal issues.

Finally, in-house counsel can oversee compliance monitoring mechanisms, making sure that the organization's internal practices align with external legal requirements. This includes not only routine compliance audits but also real-time monitoring of AI initiatives to ensure they operate within the boundaries of the law and ethical norms.

In sum, in-house counsel's role in navigating the complexities of AI and data is vital. By taking a proactive stance on legal challenges and working closely with other departments, in-house counsel can ensure that the organization not only complies with current laws but is also prepared for future legal evolutions.

## About the author

**Anup Iyer** is senior counsel with **Moore & Van Allen**. He specializes in assisting clients with obtaining patent and trademark rights across diverse technology sectors such as artificial intelligence (AI), optical communication, high performance computing, computer processor architecture, wireless communication technologies, and cybersecurity. He is based in Charlotte, North Carolina, and may be reached at anupiyer@mvalaw.com.

**This article was first published on Reuters Legal News and Westlaw Today on January 19, 2024.**