# CIOs face complex legal questions in governing AI projects



Enterprises aiming to deploy artificial intelligence (AI) projects face a complex landscape of legal considerations, from selecting appropriate use cases to implementing necessary compliance measures. As AI adoption accelerates, chief information officers (CIOs) must carefully navigate an evolving web of regulations across multiple jurisdictions to ensure their initiatives meet legal and ethical standards.

During a recent panel at the International Association of Privacy Professionals (IAPP) Global Privacy Summit, experts highlighted the challenges CIOs encounter in governing AI technology. Martha Hirst, an associate in the data strategy and security team at law firm Debevoise and Plimpton, emphasised the difficulty in capturing the nuanced requirements of various AI laws within governance programmes. “You’ve suddenly got to this point where all these different nuances need to be captured within governance programs, which is really hard,” Hirst remarked.

Four critical legal questions were outlined to guide CIOs in planning and executing AI projects responsibly:

1. **Is the AI use case considered high risk?**

AI implementations involving sensitive areas such as critical infrastructure, employment decisions, or biometric data are commonly deemed high risk. These use cases require particularly stringent controls to comply with anti-discrimination and other regulations. Cynthia Bilbrough, global head of HR privacy, digital and risk at GSK, noted the difficulties companies face with traditional recruiting processes amid surging job applications. She cautioned that AI-driven applicant filtering tools might inadvertently introduce bias, potentially placing companies at risk of legal noncompliance.

Leaders developing AI systems in such contexts should familiarise themselves with applicable laws mandating automated decision-making safeguards to mitigate fines and other penalties.

2. **Which jurisdiction governs the AI tool’s deployment?**

Legal frameworks regulating AI vary substantially across countries, states, and regions, creating intricacies in ensuring compliance. Christina Montgomery, IBM’s vice president and chief privacy and responsible technology officer, stated, “There’s already 140 privacy laws. We’ve got the EU AI Act. We’ve got every jurisdiction pretty much out there regulating AI at this point.”

Stephanie Westfield, senior privacy counsel at Ford Motor Company, urged organisations to avoid fragmented compliance strategies. “A siloed approach… just doesn’t cut it anymore. Now is the time to think about how you align with a global approach and find the highest watermark,” she commented, advocating for adherence to the most rigorous standards internationally.

3. **What is the nature and origin of the data used?**

The quality and provenance of data employed to train AI models greatly impact system performance and legal compliance. Brigette Guyer, global data protection, privacy and risk officer at The Wendy’s Company, described how every AI project undergoes a risk review before initiation, balancing the use of real versus synthetic data.

Synthetic data, which does not contain real personally identifiable information, can offer advantages in respecting privacy regulations like the European Union’s General Data Protection Regulation (GDPR). When generated properly, it may also diminish biases present in historical datasets.

Organisations can further enhance compliance through comprehensive data-mapping exercises, a process frequently overlooked despite its importance. Amber Cordova, AI, privacy and cybersecurity counsel at Vistra Corp., emphasised, “Be organized. Data mapping is something nobody wants to do, and yet is so important and worth putting resources into.”

4. **Should the AI solution be built internally or procured?**

Managing risks arising from third-party AI vendors requires careful scrutiny. Experts at the IAPP session highlighted the necessity of understanding how external providers use and protect data entered into their systems and what guardrails they implement to minimise biases and other risks.

Organisations are increasingly seeking contractual assurances beyond standard clauses like copyright indemnification. These provisions aim to shield companies from potential AI-related liabilities. CIOs are encouraged to collaborate with privacy teams during vendor negotiations to identify and mitigate avoidable risks linked to AI deployments.

The insights shared at the IAPP Global Privacy Summit underscore the multifaceted challenges enterprises face in harnessing AI within legal boundaries. As regulatory regimes continue to develop worldwide, CIOs play a pivotal role in balancing innovation with cautious governance to navigate an increasingly complex regulatory environment.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.ailawandpolicy.com/2024/01/artificial-intelligence-legal-issues-2023-year-in-review-and-areas-to-watch-in-2024/> - This source discusses the evolving legal landscape of AI, including state legislation and White House actions, which supports the challenges CIOs face in navigating AI regulations.
2. <https://epiloguesystems.com/blog/5-key-ai-legal-challenges/> - This blog highlights key AI legal challenges such as intellectual property disputes, data privacy concerns, liability in AI decision-making, and bias, which align with the legal questions outlined for CIOs.
3. <https://legal.thomsonreuters.com/blog/how-ai-transformed-the-legal-profession-in-2023/> - This article explores how AI transforms the legal profession by highlighting areas like compliance and liability, which are crucial for CIOs in managing AI projects.
4. <https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-april/big-data-big-problems/> - This resource delves into legal issues related to AI-driven data, including intellectual property and privacy concerns, echoing the complexity of managing data in AI projects.
5. <https://www2.deloitte.com/us/en/pages/consulting/articles/generative-ai-legal-issues.html> - Deloitte discusses the legal implications of Generative AI, including IP infringement risks and data protection obligations, which are important considerations for CIOs managing AI projects.
6. <https://iapp.org/resources/article/global-privacy-summit/> - Although not directly linking to the IAPP Global Privacy Summit article, this site provides resources related to privacy and AI governance, aligning with the panel discussions highlighted in the article.
7. <https://news.google.com/rss/articles/CBMilgFBVV95cUxOMHpwbXhVa2Vta3Bkb2FGVDR6NF9OejQ1MUE2bjBfcmxuTVo1aC1jM1FkeTJscTJnR01pT2RHRnkxcm9rUWl2NWgzZ0VXbVBSYmFvMHRfOHRUZGJOODRrU0RPRUhoR2NmTTc3YTBkc1RfbWZjc3FSWEkzMnItMm4waVBQczlhSWJNdFlnLXFHM1JxNDE3M0E?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data