**AI Accountability: Considerations for Privacy Professionals**
By Nina Bryant and Meredith Brown, FTI Technology

Artificial intelligence governance has become a priority for organizations looking to responsibly develop or deploy AI solutions and has significant potential impact for privacy professionals. The concept is often loosely defined within organizations, with many clear only on the fact that they should be doing something with AI governance, rather than what they should be doing or how to execute it across their enterprise, products and operations. Standards and frameworks for AI governance have begun to emerge — with ISO 42001 and the NIST Responsible AI Framework at the fore — and are continuing to mature as global regulation evolves. However, defining responsibility for AI governance within an organization is critical to ensure AI is implemented ethically and compliantly. This ownership is nuanced and often sits across multiple business areas in order to ensure the full range of legal, technical and compliance risks are appropriately assessed, and will likely vary depending on each organization's level of maturity and risk posture.

Any ambiguity surrounding AI accountability presents an opportunity for legal departments, and privacy officers in particular, who are poised to step in and help integrate their organization's assessment of AI projects into existing data protection and privacy practices. Given that AI tools are data-dependent and that privacy regulations govern the processing of personal data, these laws serve as primary mechanism for supporting AI governance and guiding ethical use of technologies that rely upon personal and sensitive data. By serving as an internal expert at the intersection of data privacy and AI risk, data privacy officers can partner with the general counsel and other key stakeholders to help their business pursue innovation responsibly.

Alongside their counterparts, the privacy team can help address key categories of AI accountability, particularly who may be impacted, organizational risks and ethics. Essential considerations across these areas are outlined here.

**Groups and individuals to whom the organization is accountable**

- **Employees.** If employee data is being fed into a model, or employees are using AI to do their jobs, the organization is accountable for providing usable tools that can be trusted as safe and ethical and for guiding employees on appropriate use of generative AI.
- **Customers and clients.** If customer data is being used in the model, there are a range of privacy, ethical, contractual, security and transparency considerations that will need to be addressed. As AI becomes increasingly embedded within the customer journey, clear signposts will be required to ensure transparency on where there is a human involved in the process and where AI interaction begins and ends.
- **Strategic partners and third parties.** Depending on the use case and the technology being used, there could be aspects that conflict with existing partner agreements relating to sensitive data or intellectual property. Assessing third-party

risk is a key dimension of assessing products which include AI to deliver key functionality. Additionally, missteps that result in reputational damage could likewise damage important partner relationships.

- **The board and chief executives.** The c-suite needs a strong understanding of the business strategy for AI as well as the risks and opportunities. Alignment on AI risk and governance across business functions, the c-suite and the board is critical to protecting the organization on all fronts.

These groups and individuals have rights and expectations to be informed about the ways AI systems may impact their privacy or their organization's privacy risk. Understanding what AI systems are in use, their purposes and their data sets will inevitably need to feed through to key privacy documentation, such as privacy policies, lawful basis, privacy notices and data protection impact assessments. Additionally, many privacy laws include rights for individuals to opt-out of automated decision-making underpinned by AI systems, which they can only do when there is transparency and explainability around the way AI solutions operate and how decisions are made. From data collection throughout its lifecycle, openness about the types of data collected, how it is used, the impact on data subject rights, and potential consequences of the technology will be essential. Privacy professionals can encourage accountability within their organizations to understand these nuances, even within opaque technologies, and provide transparent disclosures to internal and external audiences.

**Organizational risk**

- **Existing or impending laws that regulate the technology.** AI regulation has already been implemented in Europe via the EU AI Act, which becomes effective in August 2026 . One of the learnings from other largescale EU regulations is there is a long tail of enforcement activity and potential follow-on litigation.

  Whilst GDPR too effect in 2018, regulators were still issuing substantial fines more than five years later for approaches taken in 2018 and 2019. As such, organizations need to take a robust yet pragmatic approach to making the right decisions regarding AI now, as otherwise they may pay for poor decisions, especially relating to bias, fairness and transparency, several years from now.

  As lawmakers around the world continue to enact regulations that will govern many aspects of AI, privacy and compliance officers must navigate the complex balance of enabling progress, innovation and efficiency, whilst balancing risk to the business and individuals. Key to this will be setting an appropriate baseline level for global compliance that is easily understood and practical. Privacy officers have a wealth of experience in this space and can add value to the business through breaking down silos and enabling effective collaboration and understanding across the business to mitigate risk and design governance and control frameworks.

- **Risk assessment.** Many organizations already feel somewhat overwhelmed by the volume and complexity of existing risk management processes, from vendor due diligence to cyber assessments and data protection impact assessments. Most organizations have little appetite for adding on multiple new processes. Privacy officers can support this approach by looking to embed additional AI risk assessments and scoring within existing frameworks and processes, helping to mitigate risk with minimal impact on business efficiency.
- **The scope of personal or sensitive data that may be generated, stored or shared.** As part of assessing risk, privacy teams should inventory the personal data underlying their organization's AI systems as well as the systems themselves. Those with existing data privacy programs likely already have a robust data map of personal information flows across their organization, so these can be built upon to reflect usage within AI systems, as well as related requirements such as encryption, aggregation or deidentification. In addition, asset registers should be updated to include AI solutions, along with relevant information regarding data sources, risk levels and testing or monitoring processes. This is a core responsibility in upholding accountability, documenting and mitigating risks and enabling transparency.

**Ethical responsibility**

- **Understanding who or what might be harmed.** In the foreground, organizations will be primarily concerned with the potential for AI to harm employees, customers, partners and the company's value. Organizations must also be aware of risks such as AI-washing and avoid overstating the role AI plays in new products and services. Responsible AI is a part of the wider issue of trust between consumers and organizations. If that trust is broken, be it through data breaches or biased or unfair AI algorithms, this has an immediate impact on brand and reputation. There is an expectation from society that organizations will develop AI responsibly, consider the impact on individuals and society, and take appropriate action. For example, supporting workforce training and upskilling to avoid job losses, ensuring human-AI collaborative decision making or carbon off-setting for environmental impacts.
- **Managing bias and drift in the AI models.** Data used to train AI models and the underlying algorithms within these systems often have biases embedded in them. Unchecked, they can also drift from their intended purpose. Ensuring regular testing, fine-tuning, monitoring and proactive controls are part of a suite of governance measures to prevent introduction of bias.
- **Education to ensure appropriate use.** Employees play an integral role in maintaining strong governance. As new AI tools are deployed, employees will need to be trained on the ethics of these tools, taught how to avoid misuse and educated on the potential for harm.

Privacy teams have an opportunity to be vocal about these issues and work with their counterparts to manage them proactively. More so, privacy teams can work to establish privacy by design practices at the foundation of their organization's AI projects, which

embeds privacy policies, risk mitigation and principles of trust into new systems at the outset of development and implementation. For AI projects, this can include AI-specific risk assessment workflows, adding new controls to address gaps in privacy within AI tools and datasets, and creating approval cycles specifically for AI accountability. Privacy enhancing technologies may also be useful in automating certain steps in building privacy into AI systems and monitoring AI systems for unexpected privacy shortfalls.

Where AI systems process personal data, those with accountability for privacy will need to ensure alignment between existing policies and new AI functionality and uses. With AI governance, privacy teams have the opportunity to influence and bring the value of their experience of driving culture change in a new and important field of business strategy and innovation. They can help their organizations pursue digital transformation while staying accountable for ethical, responsible and safe pursuit of AI objectives.