Insights: Publications

5 Key Takeaways | Privacy & Technology Law Forum: Building an AI Governance Program

MARCH 6, 2025

By Amanda Witt, Ami Rodrigues, and Christina McCoy

On March 4, 2025, **Amanda Witt** of Kilpatrick, **Ami Rodrigues** of Under Armour, and **Christina McCoy** of Innova Solutions presented on how to build an AI governance program at the **Privacy & Technology Law Forum (PTLF)** for the State Bar of Georgia. The presentation provided a roadmap for organizations to establish effective frameworks that are designed to ensure ethical and legally sound AI practices.

The following are the five key takeaways from their presentation:

1. Distinguish Between AI Governance and Strategy

Understanding the distinction between governance and strategy is a critical component when advising organizations on how to implement AI within the organization. The following are the key distinctions between these concepts that will help define the scope of responsibility for individuals within the organization:

- **Governance** centers on ensuring ethical, legal, and accountable AI use. It mitigates risks, ensures fairness, and maintains compliance with existing regulations. Its key elements include policies, risk management, auditing processes, and legal oversight. Governance metrics often focus on compliance rates, fairness audits, and risk mitigation success.

- **Strategy,** on the other hand, focuses on leveraging AI technologies to achieve business objectives. It emphasizes innovation, business alignment, talent development, and resource optimization. Metrics for strategy typically revolve around return on investment (ROI), business KPIs, and successful AI adoption.

Governance is critical as it provides the necessary legal guardrails for AI implementation. However, it is equally important to collaborate with business leaders, AI engineers, and product managers to ensure the governance framework align with broader organizational goals. When designing an AI governance policy, you should ensure that the governance policies address ethical considerations while supporting strategic outcomes of the organization.

2. Choose the Right Program Structure: Embedded vs. Standalone

Organizations face a critical choice in how they structure their AI governance programs. It's important to first decide whether to build on an existing program (typically a privacy program) or create a standalone program. There are benefits and challenges to both options.

- **Embedded Programs:** Some organizations integrate AI governance into existing governance programs (typically privacy programs, but could also include data or risk governance programs), offering advantages

such as unified processes, cost efficiency, and streamlined reporting. However, embedded programs may strain existing resources who may not have the requisite AI-specific expertise. An embedded program could be perceived as having too many roadblocks that slow down AI innovation.

- Standalone Programs: If an organization creates a dedicated governance structure focused solely on AI, benefits could include individuals who have specialized knowledge in AI, tailored processes given that existing legal frameworks for AI are not as complex as other areas such as privacy, and clearer accountability for AI-specific risks. However, building a standalone program is resource-intensive and may introduce challenges related to coordination, redundancy and inconsistent risk management.

It is important to evaluate the organization's resources, priorities, and risk exposure when advising on the appropriate structure. For example, standalone programs may be preferable for organizations heavily reliant on AI, while embedded programs may suffice for those with existing privacy frameworks and limited AI use. Ultimately, the choice depends on your organization's size, the complexity of AI usage, and your capacity to manage specialized programs. For smaller or resource-constrained organizations, embedding AI governance within an existing program might be a better option. However, for organizations dealing with complex AI systems or rapid AI advancements, a standalone program may be more beneficial.

3. Craft Comprehensive Policies for Generative AI Usage

An internal policy governing the use of generative AI (Gen AI) is a cornerstone of any governance program. It's possible that an organization may develop multiple policies such as one that outlines permitted uses for all employees and one that is designed for a specific audience of employees such as developers. It is important to ensure that these policies address legal and ethical concerns while providing clear guidelines for usage. Key components of a robust internal policy include:

- Principles for safe AI use: Establish foundational rules for ethical and effective AI deployment, including transparency, fairness, and accountability.

- Scope of policy: Define whether the policy applies to generative AI, machine learning models, or algorithmic decision-making systems. It is also critical to define the intended audience for the policy and the consequences for non-compliance.

- Usage authorizations: It is advisable to categorize AI into what types of AI and use cases are prohibited, require approval, and permitted. This ensures clarity for employees regarding permissible applications.

- Areas of concern: Address specific legal and ethical risks such as intellectual property (IP), data privacy, labor and employment, and bias in algorithmic models.

- Vendor management: Include requirements for vetting vendors and aligning their practices with organizational policies.

4. Prioritize Vendor Due Diligence

The success of an AI governance program often hinges on the organization's relationships with vendors. Vendors provide critical AI tools and technologies, but improper vetting can expose organizations to compliance risks and reputational harm. An organization's comprehensive vendor due diligence processes should address the following:

- **Integrating due diligence into procurement workflows:** Make vendor assessments a mandatory step in procurement to ensure all AI solutions meet ethical and legal standards.

- **Assessing vendor reputation and financial stability:** Evaluate vendors for their track record in ethical AI practices, adherence to regulatory requirements, and overall business stability.

- **Drafting robust contract**s: Include clauses that require vendors to comply with applicable law, agree to desired provisions on ownership, provide adequate indemnities and ways to monitor performance.

5. Employee Training is Key

Employee engagement is vital to the success of any AI governance program. Without proper training and communication, even the best-designed policies may fail to gain traction. Aspects of a successful AI governance program include the following:

- **Comprehensive employee training:** Training programs should focus on educating employees about safe AI practices, compliance requirements, and the organization's specific governance policies. Metrics such as participation rates, knowledge assessments, and feedback loops can demonstrate employee buy-in and engagement. Iterative training ensures policies evolve based on employee input and emerging risks.

- **Strategic communication plans:** A communications plan ensures employees understand the purpose and importance of the governance program. Communications to employees should emphasize legal compliance, ethical AI use, and the organization's commitment to accountability. Phased communication throughout the year is recommended to maintain engagement and reinforce key messages.

By emphasizing training and communication, an AI governance team can foster a culture of compliance and accountability, reducing the risk of legal violations and enhancing overall governance effectiveness.

Final Thoughts

When building an AI governance program, it is critical to balance innovation with accountability. It is vitally important to understand the needs and resources of the organization when developing a program that will help achieve organizational AI-related goals while ensuring compliance with legal and ethical requirements.

If your organization needs assistance in creating or refining its AI governance program, the Technology, Privacy & Cybersecurity team at Kilpatrick is available to help. Our team offers deep expertise in navigating the legal and regulatory landscape of AI and privacy.

For more information, please contact
Amanda Witt: awitt@ktslaw.com.