Centre for Information Policy Leadership (CIPL) and IEEE Digital Privacy Initiative

# Policy Meets Practicality: Aligning Policy and Engineering to Support Good Privacy Design

Event Takeaways | December 2025

**Centre for Information Policy Leadership (CIPL) and**
**IEEE Digital Privacy Initiative**

# Policy Meets Practicality: Aligning Policy and Engineering to Support Good Privacy Design

## Event Takeaways

As privacy engineering plays a critical role in responding to sociotechnical challenges in personal data processing, organizations must operationalize privacy in a scalable and accountable manner. The IEEE Digital Privacy Initiative and Centre for Information Policy Leadership (CIPL) hosted a roundtable in December 2025 to discuss how internal organizational governance and public policy can together support privacy engineering and innovation. This interactive discussion was meant to bridge the gap between policy goals and technical implementation by identifying best practices, key frameworks, and scalable approaches to embed good privacy design. This followed an earlier roundtable, held in San Francisco, CA, in July 2025, which was focused on the practical challenges of developing products that respect privacy while enabling responsible and beneficial use of data. To encourage open discussion, the roundtable was conducted under the Chatham House Rule.

### 1. Privacy Governance is Shifting Toward Risk-Based Approaches

- There is growing concern that privacy as a field is relying too heavily on prescriptive controls, rather than focusing on contextual risk and practical solutions.
- Taking a risk-based approach allows organizations to:
  - Focus on implementing reasonable measures tied to actual risk exposure
  - Identify gaps and anticipate threats, including those associated with AI
  - Balance privacy objectives with both business and societal benefits
- Developing functional use cases associated with threat models can increase organizational understanding of risk, identify reasonable tradeoffs when evaluating privacy objectives, and provide potential metrics for review.

### 2. Privacy, Security, and AI Governance Are Rapidly Converging

- Many organizations are moving away from treating privacy, cybersecurity, and AI governance as separate domains and are recognizing that they all play a role in facilitating good data governance.
- AI is accelerating this convergence because it fundamentally alters how data is used. When AI is integrated into a system, the context and purpose of data use can change, which can create new privacy risks.
- As a result, many organizations are building their AI governance on top of established privacy or data governance frameworks, rather than creating new, separate processes, which can reduce internal friction and confusion.

**3. Strong Data Governance is the Foundation of Responsible AI**

- Effective development and adoption of AI is only possible with good data governance and should be supported internally through training and education (e.g., of AI-related risks and threats, relevant compliance or regulatory requirements).
- Some examples of good data governance include:
  - Clearly mapping data assets and understanding how they are used
  - Classifying high-risk or highly sensitive data elements (e.g., Social Security numbers)
  - Identifying the value and risks of data elements
- Good data governance also considers the role of vendors, and organizations should still govern third-party use of data, such as documenting data provenance and usage through a "data bill of materials".

**4. Privacy Must Be Embedded Early in Product Development**

- It is critical to integrate privacy from the earliest stages of product and policy design as it will only become more difficult to do so as product design or development progresses.
- Organizations should identify points in the standard product development lifecycle to embed privacy risk assessments and implementation of mitigation measures, including:
  - Product or service design and ideation
  - Development and testing
  - Change management processes
- Frameworks like the NIST Privacy Framework can serve as useful tools for organizational privacy and engineering practices. The NIST Framework can also assist with identifying relevant data and mitigating data risks as well as developing cross-organization communication (e.g., engaging engineering teams, fostering ways to prepare for and respond to regulatory requests).

**5. Translating Privacy Principles into Operational Practices**

- Organizations must be able to translate high-level legal principles into actionable requirements for engineering and product teams.
- To achieve effective data governance, in-house attorneys are having to serve as both translators, communicating legal and compliance requirements in plain language, and diplomats, meeting teams where they are and engaging with key stakeholders to help embed privacy into their workflows.
- Practical strategies to help elevate privacy as an organizational priority include:
  - Creating short guidance documents that outline current privacy issues, regulatory trends, company priorities and principles, and practical action items

- Translating legal obligations into clear engineering requirements
- Engaging with teams through familiar or easily accessible modes (e.g., team communication channels, internal knowledge platforms)
- Tailoring training for specific teams or audiences

**6. Organizational Ownership of Privacy Must Be Distributed**

- Privacy cannot be effectively managed by a single centralized team, and organizations should consider how to individualize ownership of privacy throughout the organization so that privacy responsibility is shared.
- Examples of best practices include:
  - Appointing privacy or security leads within business units
  - Building networks of privacy "champions" that act as designated points of contact for privacy-related questions
  - Clearly distinguishing between those responsible for setting the policy vs. those responsible for implementing the policy decisions
  - Establishing an escalation path and determining how information will be presented for executive management decisions
- Some emerging regulations may require senior leaders or board members to testify in privacy cases (e.g., California). This could provide opportunities for organizations to elevate privacy issues at the executive level.

**7. The Importance of Shared Taxonomies and Definitions**

- A common taxonomy is essential to ensure that different business units are able to interpret and apply key terms in a consistent manner. This is especially important for data and risk assessments.
- Organizations should clearly define relevant terms and even consider hiring a dedicated taxonomist.

**8. Incentives and Metrics can Strengthen Privacy Programs**

- Organizations are increasingly exploring ways to support privacy program implementation with clear incentives and performance metrics throughout all levels of the organization levels.
- Some examples of best practices include:
  - Integrating privacy metrics or scorecards into performance reviews, especially at the directors or team lead level
  - Rewarding engineering teams that meet privacy requirements as part of producing a viable product
  - Conducting quantitative evaluations of privacy benchmarks to assess why objectives are not being met and highlight potential gaps in operations, engineering, etc.

- These mechanisms can help shift the perception of privacy as a compliance burden to being a core component of building trustworthy, safe products.

**9. Developing Effective Privacy Communication and Training**

- Traditional privacy training programs, such as annual training, are no longer sufficient to cover the complexity of current data and privacy issues.
- There is a greater need for more targeted training and communication strategies, including:
  - Tailoring training sessions to consider the unique responsibilities and challenges of specific business units
  - Distributing privacy updates through the tools and communication channels already in use or familiar to specific teams
  - Providing regular internal benchmarks of company positions on privacy-related topics
  - Developing videos to recreate privacy scenarios for training purposes

**10. Managing Vendor and Third-Party AI Risks**

- AI has significantly increased the importance of vendor and third-party governance. Organizations are often encouraged to trust AI vendors, yet their principles may not align with the internal policies.
- Thus, organizations should ensure that any vendor's practices align with their own internal privacy and governance standards. This can be achieved through thorough vendor assessments that consider:
  - Data classification, processing, and storage
  - Data provenance
  - Privacy and AI governance issues
- Procurement teams should be included in any discussions and decisions involving vendors or third-party partners.
- Ultimately, data and AI governance responsibilities cannot end when data leaves the organization, and these considerations should be reflected in any vendor or third-party assessments.

**11. Reconsidering the Effectiveness of Notice and Consent**

- Traditional notice-and-consent models may no longer be effective in empowering users to make informed choices.
- Although consent has remained a central element of many global policy regulations, users often click "agree" to access digital services they need without fully reading or understanding what they are consenting to.
- Organizations have explored alternative approaches that could potentially provide users with more control, such as:

- Clearer user options, like "do not share my data"
- Stronger privacy thresholds that can allow users to assume foundational safety of a product/service
- Considering what is fair to the user and place the user as a central stakeholder into product discussions

**12. Considering a Harm-Based Approach to Privacy Regulation**

- If greater user control is not possible, we may want to collectively consider the role of a "harms-based approach", which would require regulators or policymakers to define what constitutes harm and establish an acceptable risk threshold for digital products/services. However, meaningfully assessing risk to a single user remains challenging as there is no widely accepted definition of what is considered "safe."
- There is also a question of whether current regulations are sufficient to mitigate or prevent harms, or if new laws are necessary. For example, California has added new privacy requirements to its laws that have driven adoption of new privacy design practices.
- Current remedies for user harm also need to be reevaluated. For example, is offering access to a free credit report service for one year an equitable exchange for the harm caused by the loss of someone's personal data? There is a need for increased incentives for companies to acknowledge risk and provide appropriate remedies to individual users. Many large companies have insurance policies, and higher costs are driving some to implement improved privacy policies.

**13. New Policy Tools for Privacy Innovation**

- Emerging policy tools can improve privacy protections, while balancing technological innovation. Examples include:
  - Privacy labels or scoring systems similar to nutrition labels
  - Developing universal language or symbols to increase user awareness
  - Performance-based standards that require disclosures on how the product/service met or failed to meet basic user safety thresholds
  - Regulatory sandboxes that allow organizations to test new technologies under regulatory supervision
- Broader public awareness campaigns and partnerships between industry and regulators may help drive meaningful change in privacy protections. For example, a guideline created with both public and private input that helps parents understand risks to minors and clearly outlines when a product cannot be marketed to certain age groups.

**14. Cross-Functional Collaboration is Essential**

- Effective privacy governance ultimately requires strong collaboration internally across organizational functions and externally with relevant stakeholders (e.g., regulators, civil society, general public).
- Privacy teams should work closely with engineering, product, marketing, legal, and executive leadership and should create opportunities for learning exchange, such as:
    - Building cross-functional teams and embedding "privacy champions"
    - Getting early feedback from teams on new processes or tools (e.g., changes to risk assessments)
    - Demonstrating how privacy programs can lead to tangible return on investment (ROI)
    - Building guidelines for new privacy measures
    - Effective internal change often depends more on building sustainable relationships than on legal requirements alone, and privacy initiatives should be able to demonstrate return on investment (ROI)
- By framing privacy as a shared mission to build trustworthy products and services, organizations can foster a culture that prioritizes responsible data stewardship and ethical technology development.

## Additional Resources

Center on Responsible AI and Governance (CRAIG)

IEEE Digital Privacy Model

NIST Privacy Framework

Data Privacy: A runbook for engineers

CIPL-Cisco Report on Business Benefits of Investing in Data Privacy Management Programs

## Thank you to our participating organizations:

Adleman Consulting Services, LLC

Adobe

BDO

CableLabs

Centre for Information Policy Leadership (CIPL)

Cisco Systems, Inc.

Deloitte

Elasticsearch

Fanduel

National Institute of Standards and Technology (NIST)

Google

IEEE Digital Privacy

JLINC Labs

Meta

Ohio State University

Paramount

PRIVO

SAP

Strategai Consulting, LLC

TikTok