Centre for Information Policy Leadership
HUNTON

# From Here to Eternity: Foundations for Future-Ready Data Policy and Organizational Governance

## Takeaways from CIPL 2025 Annual Summit

March 4-5, 2025

# From Here to Eternity: Foundations for Future-Ready Data Policy and Organizational Governance

**CIPL 2025 Annual Summit**

Washington, DC

March 4-5, 2025

CIPL held its Annual Executive Summit in Washington, DC on March 4-5, 2025. With more than 100 attendees, it was CIPL's largest Summit ever. Participants included leaders from CIPL member companies, regulators and policymakers from a range of jurisdictions, and experts on data and technology policy from academia and the private sector. Both days of the Summit were held under the Chatham House Rule. The conversations and networking opportunities generated a wide variety of insights. This document highlights key themes and observations from the discussions.

## 1. Change and Disruption

We are in a moment of profound technological and political change. Policymakers, regulators, and business leaders are facing the challenge of building a path toward **"future ready" public policy and data governance practices** that facilitate and support emerging technologies.

Globally, there is an emerging dichotomy between **"deregulation"** in AI policy and creating prescriptive legal and regulatory frameworks for AI. This is playing out on an international level, e.g., EU and China supporting regulation, while the U.S. is favouring a "deregulation" or "light touch" approach, as well as domestically in the US between prescriptive state AI laws and an emerging federal approach that seems to de-emphasize regulation. Regardless of regulatory approach, there seems to be a shared perception that there is a paradigm shift, or a shift in focus, from merely managing risks as they arise to facilitating innovation through proactive efforts.

## 2. Increased Relevance of Key Areas of CIPL Work

When organizations prioritize the **responsible use of data** and its societal benefits, it spurs innovation in a way that protects the privacy of consumers. Bad data leads to inaccurate predictions and creates a business risk, and poor data use creates a bad customer experience and leads to legal risks. **Organizational accountability** remains a durable business enabler, despite shifting policy and regulatory priorities. Businesses thrive in an environment where **smart regulation** provides consistency and certainty. This flexible, risk-based approach builds on existing laws and standards and incentivizes best practices and organizational accountability.

## 3. Holistic Data Management and Oversight to Foster Digital Trust

Organizations' data governance leaders are seeing their **roles evolve** within this rapidly shifting landscape. Their

focus has shifted beyond privacy to a more holistic conception of data governance that encompasses compliance, but within the broader objective of identifying how **data can be a source of business value**. They are constantly weighing the right balance among risk, trust-building with customers and partners, and the speed of innovation and technological adoption. **Key performance indicators**—both qualitative and quantitative—are essential for measuring success.

A holistic data strategy breaks down the silos between the different departments working on data (i.e., privacy, security, research and development, etc.) to **foster collaboration** and develop a unified approach to data management. It is important to align data initiatives with company values and business ethics.

Building and maintaining digital trust to enable sustainable and competitive digital business is essential; however, **measuring digital trust is difficult**. Key performance indicators (KPIs) must shift from a narrow focus on compliance metrics (such as avoidance of fines) to those that address a broader range of indicators of value, such as support for growth of new business.

## 4. Balancing Risks and Benefits of AI

AI can play a vital role in helping solve both business and societal problems, but achieving optimal performance while addressing ethical considerations and risks requires **careful consideration and deliberation on impacts.** Organizations should incorporate a range of perspectives in risk assessment processes that sufficiently reflect the relevant stakeholders impacted by the technology. Every design choice in an AI tool is ultimately a normative decision.

## 5. AI Agents and the Next Wave of AI Innovation

**AI Agents** have tremendous potential to increase productivity and optimize processes for organizations and individuals. These new technologies can offer more robust privacy protections but also pose new challenges for ethical governance with respect to individuals and society. Organizations must tailor governance to address both agent-to-agent and agent-to-human interactions. Potential risks of this new technology could include: goal misalignment, e.g., improving sales vs. inadvertently producing misleading/false information, e.g., agent-to-agent, agent-to-human, agent-to-environment interactions; workforce displacement; human impact in the form of disempowerment and disengagement. Robust data governance will be essential for successful agent deployment, and organizations will not be able to realize the full value of their data without good data governance. Thus, organization with thoughtful data governance practices, then you will get a better output from AI agents. Certifications may also play an important role in facilitating trustworthy agentic AI.

## 6. Shifting Geopolitical Landscape

The **rapidly changing geopolitical environment is having sweeping impacts** on public policy around AI, technology, and data.  Geopolitics used to be the sphere of nation-states exclusively, but now private sector organizations play a major role. Governments are now acting by and through private companies – how should companies behave when governments are viewing them as instruments of power?

**"Sovereignty"** has been an animating theme of technological competition between countries in recent years, and it continues to be relevant even as jurisdictions explore avenues for cooperation. Digital sovereignty policies can create both opportunities and challenges for organizations as they seek to do business across borders and position themselves as trustworthy service providers. The movement toward sovereignty has created competitive tensions even among friendly countries.

The U.S., the EU, and China remain leaders in global discussions on AI governance and each strives to lead in the development and deployment of AI. However, **the AI landscape is increasingly multi-polar**, as other jurisdictions make their mark with respect to technological development and deployment, policy, and regulation.

Global discussions on AI ethics, safety, and responsibility seem to be evolving toward a focus on **"AI security,"** although the meanings and distinctions among these terms are contested. Ultimately, responsible and trustworthy AI are key elements of secure AI. Furthermore, these elements are crucial for fostering trust with consumers, business partners, and regulators, and thus, good for business.

**Cross-border data flows** remain vital for technological development and a range of business and societal benefits and the "AI race" significantly requires cross-border data transfers. That said, we are in a moment of uncertainty with respect to the legal instruments and diplomatic arrangements that enable them.

**Durable solutions for trustworthy data flows** are essential – whether through modifications to existing bilateral and multilateral arrangements, or new approaches altogether. The Global CBPR and Global PRP frameworks are a promising option, but they need to resolve the government access issue. Outdated and overly restrictive and cumbersome data transfer legal regimes (e.g., GDPR-like adequacy mechanisms) may have to be updated. Restrictive data transfer regimes may also become the targets of countermeasures based in trade policy.

## 7. Regulators of the Future

### i. Global Shift in Regulators' Approach to Privacy, Data, and AI

**Data protection authorities around the world are striving to meet the moment**. They are trying to enable the use of beneficial technologies while protecting individuals from harm. Forward-thinking regulators are engaging with technologists in order to better understand emerging technologies.

Regulators are striving to **foster coherence in regulating privacy, data-use, and AI** across regulatory bodies (including non-privacy and data protection regulators) within jurisdictions as well as across borders. Cooperation must be multi-level, extending from joint statements by senior officials to interactions among working-level staff on the details of implementation. Regulators must also meet the "pacing challenge" and be "highly adaptive" in the face of quickly evolving and emerging technologies (e.g., quantum computing, neurotechnology). There is no escape from new technologies. To meet the regulatory challenges posed by fast-paced technological development and evolution, one regulator is considering an experimental regulatory environment to evolve laws and regulations in a way that fosters proper incentives.

## ii. U.S. State Privacy Legislation and Enforcement

Across U.S. states, **Attorneys General are working closely together** to clarify key concepts and align approaches to interpretation and enforcement under state privacy laws. Strong cooperation among AGs helps make the "patchwork" of U.S. state privacy laws a more seamless quilt as they seek to align enforcement priorities and legal interpretations.

Some state AGs are exemplifying practices of smart enforcement long championed by CIPL, such as investing in proactive education and engagement with regulated entities; maximizing beneficial outcomes by encouraging entities to put in place effective and **accountable governance** programs; and being "**selective to be effective**" by focusing enforcement actions on willfully bad actors.

**U.S. state legislators** continue to propose new legislation on privacy and AI, with the latter increasing at an especially rapid pace. Legislators are sensitive to concerns about inconsistencies across state laws and are seeking to identify ways to improve upon legislation already adopted in other states without complicating compliance or lessening interoperability. This is a challenging task.

## iii. U.S. Federal Privacy Legislation

Meanwhile, the **U.S. Congress** is again taking steps toward federal privacy legislation, with lawmakers on the U.S. House of Representatives' Energy and Commerce Committee launching a working group to study key concepts for a new law. If Congress adopts a federal privacy law, this could slow momentum on states passing privacy laws of their own.