iapp

Built to Scale: Privacy and AI Risk Frameworks

Tuesday, 24 June 2025

10:00–11:00 PDT
13:00 –14:00 EDT
19:00–20:00 CEST

Welcome and Introductions

Panelists

Gail Krutov
Sr. Privacy Counsel
BigID

Aaron Weller
Leader, Privacy Innovation & Assurance
HP, Inc.

Agenda

- Global AI Legislative Landscape
- Highlighting Key AI Laws, Regulations and Frameworks
- Building Scalable AI Governance
- AI Assessments
- Balancing Innovation and Risk
- AI Trends and Predictions
- Key Takeaways

Where do we Stand in 2025

This map shows which jurisdictions are in focus and covered by this tracker. It does not represent the extent to which jurisdictions around the world are active on AI governance legislation.

Jurisdictions in focus

Argentina • Australia • Bangladesh • Brazil • Canada • Chile • China • Colombia • Egypt • EU • India • Indonesia • Israel
Japan • Mauritius • New Zealand • Nigeria • Peru • Saudi Arabia • Singapore • South Korea • Taiwan • United Arab Emirates • U.K. • U.S.

Navigating the AI Legislative Landscape

AI legislation is rapidly evolving, creating a complex, fragmented, yet interconnected global patchwork.

Key categories of AI laws and regulations:

- Comprehensive (e.g., EU AI Act)
- Sector-specific (e.g., healthcare, finance, employment)
- Generative AI-focused
- Data/privacy-centric provisions
- Ethical guidelines and voluntary frameworks (e.g., NIST AI RMF)

Deep Dive into Key AI Laws

Key AI Laws / Frameworks to be aware of as a privacy professional:

1. **EU AI Act** - set the tone for AI laws by establishing a risk-based framework that prioritizes transparency, accountability, and ethical AI development. Its alignment with the GDPR underscores the importance of integrating privacy protections into AI systems.
2. **Australian Government 2023 AI Framework** - stricter regulation of automated decision making and profiling. Emphasizes privacy by design and compliance with existing privacy laws.
3. **Californian General Artificial Intelligence: Training Data Transparency Act** - requires transparency of datasets used to train models
4. **Colorado Artificial Intelligence Act** - aims to protect individuals from risks associated with algorithmic discrimination and requires AI assessments
5. **New York City Local Law 144** - requires employers who use AI for hiring to subject AI systems to bias audits regularly.

Building Scalable AI Governance

Building robust AI governance is essential to mitigating risk and enabling responsible innovation at scale.

Key pillars and best practices:

- Clear policies + procedures
- Cross-functional committee(s)
- Data mapping and AI inventories
- Assessments (including risk triage)
- Training and awareness

AI Assessments: Layers of the Onion

AI systems are dynamic. A “one and done” assessment is insufficient.

You can view the AI assessment as an onion, with several layers:

- Core layer: initial use case approval
- Layer 2: scope creep/feature expansion
- Layer 3: data drift/model performance (accuracy and fairness)
- Layer 4: integration and interoperability (expanded data sharing)
- Outer layer: user behavior and shadow AI (uncontrolled data exposure)

Managing Risk While Enabling Business

"We are not in the business of blocking…if this is never going to be approved, how can we get to that within 5 minutes without wasting more time?"

Focus needs to be on rapid risk identification and mitigation. Strategies to accomplish this may include:

- Upfront risk triage and categorization
- Standardized assessments
- Guardrails, not gates approach
- Clear communication and feedback loops
- Early engagement

Evolving with AI Trends

AI laws are emerging from various angles, each impacting privacy in unique ways, requiring a holistic and adaptive approach.

Some trends practitioners should anticipate include:

- Agentic AI on the rise
- Increased integration of generative AI and multimodal AI
- Growing emphasis on AI governance and responsible AI

Key Takeaways

Important steps to take (if you haven't already):

- Conduct an AI inventory
- Review and adapt internal policies, standards and procedures
- Foster cross-functional collaboration
- Invest in continuous learning
- Champion responsible AI

Questions & Answers

Panelists

Gail Krutov
Sr. Privacy Counsel
BigID

Aaron Weller
Leader, Global Privacy Engineering
Center of Excellence
HP

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/ACtQeZ6E9N

Thank you in advance!

For more information: www.iapp.org

Attention IAPP-certified Professionals:

This IAPP web conference may be applied toward the continuing professional education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org