



Navigating Privacy in AI: Insights for Data Privacy Day 2025

Tuesday, 28/January/2025

08:00-09:00 PST

11:00-12:00 EST

17:00-18:00 CEST

Welcome and Introductions

Panelists



Jim Sturm
Chief Privacy Officer
Inspire Brands



David Ray
Chief Privacy Officer
BigID

- 1. Global View of AI Legislative Developments**
- 2. Highlighting Key AI Laws**
- 3. Compliance Trends in AI Laws**
- 4. CPO Fireside Chat: Establishing an AI Governance Program**
 - a. Roles in the AI Ecosystem**
 - b. Key Components of an AI Governance Program**
- a. What's Next? 2025 AI Predictions**

Where do we stand in January 2025?



US:
AI Executive Order

Canada:
AI & Data Act, June 2022 - reduce risks and **increase transparency**

China:
Draft AI Regulation

European Union:
Comprehensive AI Act
AI Liability Directive

Singapore:
AI Verify - toolkit to ensure compliance with **AI ethics**

Brazil:
Comprehensive AI Bill

Jurisdictions in focus

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

Highlighting 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.

Compliance Trends in AI Laws

AI Laws reflect a growing emphasis on transparency, accountability and individual control over personal information processed by AI systems. These themes often seem to pull directly to privacy principles established by global laws and frameworks.

1. Transparency and Explainability

- Organizations need to be able to explain how AI systems make decisions.
- Individuals should be able to understand how decisions that affect them are made.

2. Data Minimization and Purpose Limitation

- As required under privacy laws, companies must limit the collection of personal information by AI to what is truly necessary for its intended purpose.
- The EDPB recently confirmed that legitimate interest is a valid legal basis for AI model training and development

3. Bias

- AI models must be trained on diverse datasets while ensuring sensitive data isn't used to perpetuate discrimination.

Compliance Trends in AI Laws Continued

AI Laws reflect a growing emphasis on transparency, accountability and individual control over personal information processed by AI systems. These themes often seem to pull directly to privacy principles established by global laws and frameworks.

1. Assessments

- Similar to privacy laws, assessments of AI systems must be conducted for privacy, security, and bias risks prior to deployment.

2. Data Subject Rights

- Individuals must be able to opt-out of automated decision making.

3. Security Controls

- Strong technical and organizational controls need to be implemented to protect data processed by AI systems.

4. Contractual Requirements

- Proof of Concept (++)
- (Large) Vendor agreements

CPO Fireside Chat: Establishing an AI Governance Program

CPO Fireside Chat: Roles in the AI Ecosystem

What is AI?

- There are different types of AI. Not all AI is generative.
- Definition of an AI system: Models + data + use

What are the main roles under the EU AI Act?

- Provider (technical creator)
- Deployer (implementer, maintains oversight)
- Collaborative roles bridging deployer and provider (UX/UI designers, auditors)
- Other roles include importers, distributors

What are the broader organizational roles in the AI ecosystem?

- CDO, CISO
- Head of Data Science, Chief Technology Officer
- Finance, HR, Commercial / Marketing

CPO Fireside Chat: Key Components of an AI Governance Program

Standing up an AI Governance program is key to ensuring compliance with the multitude of AI laws being passed and going into effect. This includes:

1. Creating an **AI Governance Committee** made of cross-functional stakeholders.
2. Leveraging general **frameworks** to define program controls:
 - NIST AI Risk Management Framework (AI RMF)
 - ISO 42001 Standard (Artificial Intelligence Management System)
3. Defining permitted and restricted **use cases**, aligned with a recognized **risk tiering** framework.
 - For example, the EU AI Act defines 4 risk classifications: minimal, limited, high, and unacceptable
4. Operational tasks, including conducting implementing controls, creating policies, standards, and training, and completing **AI Assessments** prior to launches.

What's Next? 2025 AI Predictions

1. **Stricter compliance standards**, including clear guidelines around ethical use of AI. These standards will likely focus on transparency, privacy, and accountability.
2. **Increased focus on showing RoI**, as organizations will prioritize measurable business outcomes and efficiency gains to justify continued investment in AI technologies.
3. **Global regulatory alignment**, fostering international cooperation to prevent regulatory fragmentation and facilitating cross-border AI applications.
4. **Stricter privacy rules**, including on the collection, storage, and use of personal information by AI systems.
5. **Enforcement actions**, likely targeting highest risk systems.
6. **Auditing and certifications of AI models** required to demonstrate that they meet regulatory standards.

Questions and Answers

Panelists



Jim Sturm
Chief Privacy Officer
Inspire Brands



David Ray
Chief Privacy Officer
BigID

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/ACtQeZ41i0>

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your 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