



Risks & Rewards of AI Laws and Regulations

Tuesday, 29 October 2024

08:00-09:00 PST

11:00-12:00 EST

17:00-18:00 CET

Welcome and Introductions

Panelists



Aaron Weller
Leader, Privacy
Innovation &
Assurance
HP



William Long
Partner, Global Chair
of Privacy and
Cybersecurity Practice
Sidley Austin



David Ray
Chief Privacy Officer
BigID

1. Overview of AI Regulations
2. Key Domains Included in AI Laws
3. Roles in the AI Ecosystem
4. Key Components of AI Governance
5. Risks of AI Laws and Regulations
6. Rewards of AI Laws and Regulations
7. What's Next? 2025 AI Predictions

Where do we stand in 2024



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.

1. Intellectual Property

- Who owns AI-generated works?
- How do we manage AI's use of existing copyrighted materials for training?

2. Data Privacy and Protection

- How can we balance innovation with data privacy?
- Can users know how their personal data is used by AI systems, and can they opt out?

3. Bias and Discrimination

- How do we prevent AI from perpetuating existing inequalities?
- How can AI systems be audited for bias?

4. Accountability and Liability (furthered by AI Liability Directive)

- Who is liable when an AI system makes a mistake - developer, user, or company deploying it?
- How do we handle instances where AI decision-making is opaque and no one can explain the cause of failure?

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 roles in the AI ecosystem?

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

Key Components of AI Governance

- 1. AI Governance Committee**
- 2. Leverage general frameworks:**
 - INIST AI Risk Management Framework (AI RMF)
 - SO 42001 Standard (Artificial Intelligence Management System)
- 3. Use Cases and Risk Tiering**
 - EU AI Act defines 4 risk classifications: minimal, limited, high, and unacceptable
- 4. AI Assessments + Control Implementation**
- 5. Monitoring / Policies**

Risks of AI Laws and Regulations

1. **Stifling innovation and economic growth:** laws may limit the ability of companies to experiment with new AI technologies
2. **Regulatory overload and fragmentation:** companies might face complex, overlapping laws across different countries, increasing the burden of compliance and legal risks and potentially making a global rollout of a new AI technology impossible
3. **Lack of flexibility in rapidly evolving space:** laws that are too rigid may become outdated quickly given the rapid evolution of AI, resulting in a slowdown of future AI advancements
4. **Barriers to entry for small players:** compliance with laws can be costly and resource intensive, making it difficult for small companies and startups to compete with larger companies
5. **Slower deployment of beneficial AI:** compliance with laws could delay rollout of AI technologies with societal benefits (e.g., healthcare, energy) due to lengthy approval processes

Rewards of AI Laws and Regulations

1. **Promoting ethical AI development:** laws help ensure that AI technologies are developed and used in ways that align with societal values, promoting fairness, transparency, and accountability
2. **Preventing harm:** laws can mitigate risks such as biased decision-making, discrimination, and unsafe AI applications
3. **Building public trust in AI:** by ensuring transparency and accountability, laws can foster public trust, encouraging wider adoption of AI technologies by reducing fear and skepticism
4. **Safeguarding privacy and security:** laws ensure that data collection complies with privacy laws and that AI systems are built with security by design principles
5. **Encouraging responsible innovation:** laws provide a framework that encourages innovation in a responsible way, promoting research and development while ensuring AI is used for beneficial purposes

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



Aaron Weller
Leader, Privacy
Innovation &
Assurance
HP



William Long
Partner, Global Chair
of Privacy and
Cybersecurity Practice
Sidley Austin



David Ray
CIPP/US, CIPM, CIPT
CPO
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/ACtQeZ39zz>

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