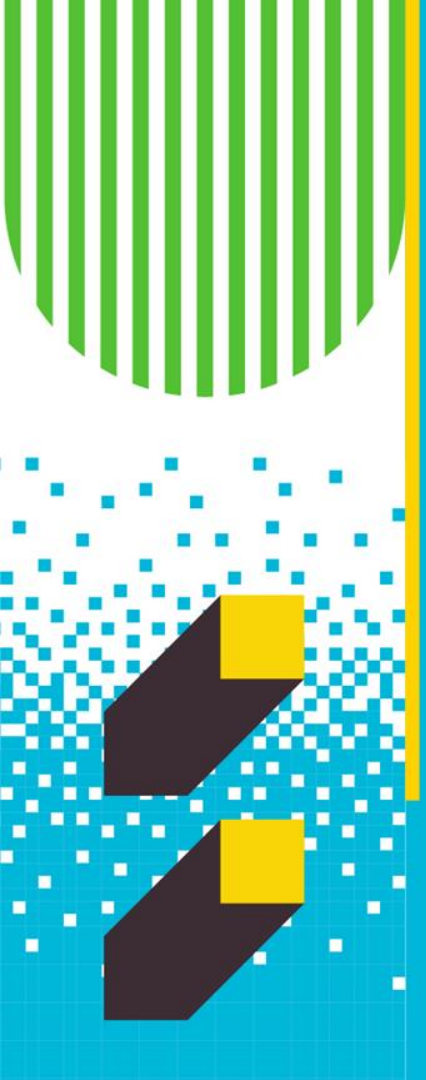


IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

An Interdisciplinary Approach to AI Development and Regulation

Robyn Eckerling, Matthew F. Ferraro, Shannon Togawa Mercer, and Ali Jessani

Speakers

Robyn Eckerling
Chief Privacy Officer, Tempus
robyn.eckerling@tempus.com

Ali Jessani
Counsel, WilmerHale
ali.jessani@wilmerhale.com

Shannon Togawa Mercer
Senior Counsel, OpenAI
stm@openai.com

Matthew F. Ferraro
Partner, Crowell & Moring
mferraro@crowell.com

Agenda Outline

- Overview of AI (including related concepts)
- Governments' Approaches to Regulating AI
- AI Considerations from the Developer Perspective
- AI Issues from the Deployer Perspective
- Navigating AI Issues as Outside Counsel
- Key Takeaways
- Questions

Early Foundations: 1940s-1950s

- "Turing Test" - a simple evaluation to determine if a machine could convincingly imitate human intelligence

Birth of AI: 1956

- Officially founded in 1956 at the Dartmouth College workshop, where the term "artificial intelligence" was coined. Early computers demonstrated the ability to solve algebra problems, learn English, and play checkers—astonishing feats for the time.

Key Milestones in AI Development

- 1966: ELIZA and Natural Language Processing (NLP)--ELIZA was one of the first programs to simulate conversation using pattern matching and substitution, marking the birth of NLP. While ELIZA gave the illusion of understanding, it did not truly comprehend language.
- 1997: AI Outperforms Humans–IBM's Deep Blue defeated the world chess champion, demonstrating that AI could outperform humans in complex, rule-based tasks.
- 2012: The Power of Deep Learning–AlexNet's victory in the ImageNet competition showcased the power of deep learning and neural networks, enabling machines to learn complex relationships in data.
- 2022: Generative AI Breakthroughs–The release of ChatGPT captured public interest, demonstrating the capabilities of large language models (LLMs) to generate human-like text and perform a wide range of tasks.

AI has evolved from simple rule-based systems to sophisticated models that learn from data:

- **Machine Learning (ML):**
  ML enables computers to find hidden relationships in data and build models to predict outcomes. It's about teaching machines to "learn" from examples.
- **Deep Learning:**
  A branch of ML that uses neural networks with many layers, mimicking the human brain's structure. Deep learning allows for the discovery of deeper, more abstract patterns in data.
- **Generative AI:**
  The latest evolution, generative AI uses large language models trained on vast datasets to understand and generate new content. These models can detect abstract patterns and create text, images, and more.

At its core, AI is a pattern predictor. While terms like "learning" are used, it's important to remember that AI generates outputs based on patterns in the data it has seen—it can be a very good predictor, but it can also be wrong.

Different Approaches to AI Regulation

- Comprehensive (EU, Certain U.S. States)
- Risk-Based (EU, Korea)
- Sector-Specific (U.S. States)
- Compute-power Based (California, maybe New York)
- Principle- or Framework-Based (NIST, OECD)
- Sandboxes (Texas, federal law pending)

U.S. AI Regulation

Kaleidoscope of law-making and rulemaking

- Federal legislature & Federal regulators; State legislatures & State regulators; International regulators; Plaintiffs' bar/Suits

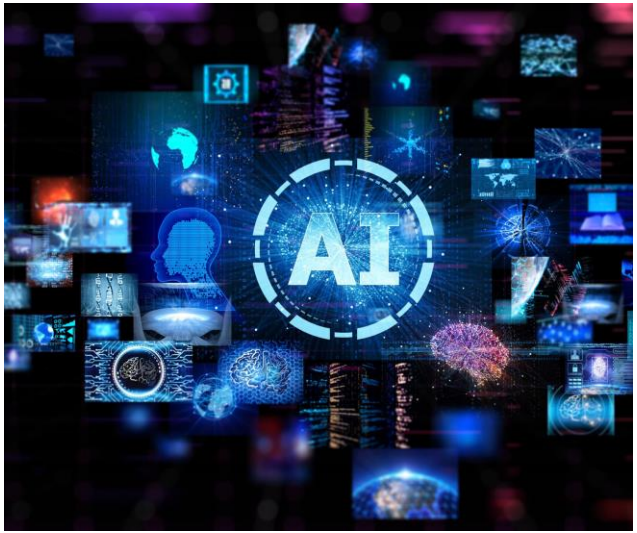
Patchwork state landscape

- A number of states (e.g., California, Texas, Arkansas, Colorado) are passing legislation regulating the use of AI, including (in some cases) specific security requirements.
- The U.S. Senate did not seek to preempt state laws or to pass a "moratorium" last term, keeping the locus of AI lawmaking in the states.

Federal movements

- For several years, federal agencies have used existing law to regulate AI and cybersecurity (including FTC Act and False Claims Act - Cyber Fraud Initiative).
- The Trump administration passed the TAKE IT DOWN Act, rescinded prior executive orders, and released a 103-recommendation AI Action Plan focusing on innovation and infrastructure

President Trump's AI Strategy Overview



- President Trump has expressed a preference for innovation, adoption, and deregulation. But that does not tell the entire story.
- Push to remove "burdensome" regulation competes with other Administration initiatives:
  - Ban on procurement of "woke" AI.
  - Active promotion of certain exports and certain data center constructions.
  - Export fees on semiconductor.
  - Stake in semiconductor company.
  - Focus on cybersecurity and other risks redolent of Biden Administration policies.
- Federal regulators pressing ahead with investigations.

AI Action Plan Summary

- Plan is structured around three pillars:
  - Accelerating AI Innovation
  - Building U.S. AI Infrastructure
  - Establishing U.S. Global Leadership in AI Diplomacy and Security
- Plan does not have the force of law & does not endorse a moratorium on, or federal preemption of, state AI laws and does not assert that training AI on copyrighted data constitutes "fair use."

- Calls for RFI to identify Federal regs that hinder innovation. Comments due 10/27.
- Recommends FTC review prior investigations, dispositions that burden AI.
- Recommends OMB withhold funding from states whose regs are "burdensome".
- Invites FCC to investigate whether state AI laws interfere with the FCC's duties.
- Suggests agencies work with industry to incorporate AI scenarios into cyber plans.
- Recommends gov "[e]valuate frontier AI systems for national security risks[.]"

Executive Orders

Infrastructure EO

- Seeks to accelerate federal permitting of data centers by making certain “Qualifying Projects” eligible for financing and expedited permitting reviews. (Qualifying Projects meet certain criteria or are designated by Cabinet secretaries.)
- Recommends streamlining environmental reviews for data centers and related energy infrastructure.
- Directs several federal agencies to identify sites for the deployment of AI infrastructure on federal lands.

Export EO

- Seeks to promote the export of an American AI technology stack.
- By Oct. 21, government is to establish “AI Exports Program” that will benefit from technical, financial, and diplomatic resources, Federal government-backed partnerships, and market access to promote export.
- Commerce is soliciting proposals from companies for packages to be included in AI Exports Program.

Ideology EO

- Seeks to prevent the government from purchasing what the administration calls “woke AI”.
- All AI procured by government must be “truth-seeking” and ideologically “neutral [and] nonpartisan.”
- OMB guidelines to be issued by Nov. 20.

Examples of U.S. State Developments

Colorado

- Restricts algorithmic discrimination.
- Requires notice to consumers.
- Imposes documentation, risk analysis obligations on high-risk AI.
- Empowers AG to bring deceptive trade practice claims.

California - Transparency Act

- Requires transparency and safety reports from developers.
- Requires explanation of potential “catastrophic risks”.
- Sets up whistleblower protections.
- Creates CalCompute.

Sector-specific Laws

- Most common sectors are those involving: chatbots (UT), nonconsensual intimate imagery (WA), political advertisements (CA), and healthcare (AZ).

AI Considerations From a Developer's Perspective

- Building beneficial technology
- Developers sit upstream
- Risk-based regulation (e.g., EU AI Act)
- Operating in a rapidly developing regulatory environment
- Developer lawyers serve as bridge between engineers and regulators, turning policy into practical controls.

AI Considerations From a Developer's Perspective

- Safety
- Security and abuse prevention
- Transparency: model documentation and limitations while safeguarding safety measures, security and IP
- Cross-functional governance: legal, policy, and technical teams coordinate on readiness decisions
- Responsible scaling
- Lawyers act as architects of trust – helping safety, compliance, and innovation move in tandem

AI Issues From a Deployer's Perspective

- Risk and Governance: Establishing control and accountability over deployed AI.
  - Regulatory Compliance
  - Governance Framework
  - Accountability and Liability
  - Risk Assessment
- Model Integrity and Performance: Ensuring the AI functions correctly, reliably, and fairly over time.
  - Algorithmic Bias
  - Lack of Explainability (Opacity)
  - Model Drift
  - Accuracy and Reliability

AI Issues From a Deployer's Perspective

- Technical and Operational Challenges: Integrating and maintaining AI within the existing enterprise.
  - Integration with Legacy Systems
  - Scalability and Infrastructure
  - Data Quality and Availability
  - Security Vulnerabilities
- Organizational and Ethical Readiness: Preparing the workforce and culture for AI adoption.
  - Talent and Skills
  - User Trust and Acceptance
  - Transparency to Consumers
  - Economic Impact

Outside Counsel Issues

- Every company is an “AI” company
- Similar to data privacy, companies are trying to figure out how to work with the patchwork of rules at the federal, state, and international levels governing AI use, development, and deployment
- AI issues fall into three buckets:
  - Policies and procedures for internal use
  - Data rights for training AI models
  - Compliance issues related to both AI use and development

Outside Counsel Issues

- Policies and procedures
  - What does an AI policy look like?
  - How are new AI-related use cases fitting into preexisting frameworks?
  - Who is responsible at the Company for AI?
- Data Rights
  - Processors want to reserve rights to train models; controllers are more affirmatively pushing back. What if the contract is silent?
  - De-identification/anonymization issues
  - Sensitive data concerns
- Compliance
  - Where does a proposed use case fit into the AI regulatory framework?
  - What about other laws?

Key Takeaways

- Perspective matters - different considerations for different stakeholders
- Everyone is trying to figure out these issues in real time
- Likely to be meaningful changes in terms of how AI is regulated going forward - industry will both drive change but also adjust
- Communication is critical (between governance and business teams especially)
- As is staying on top of new developments

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Privacy. Security. Risk. 2025**
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!