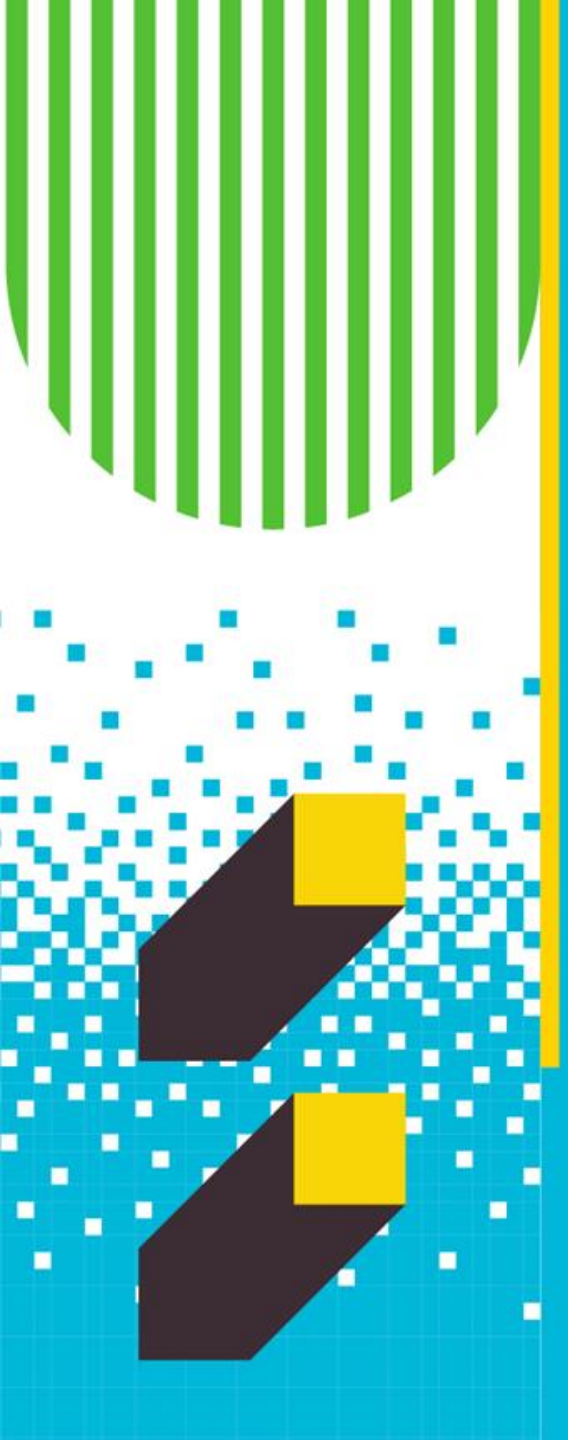


IAPP **Privacy. Security. Risk. 2025**

Training 28-29 October

Workshops 29 October

Conference 30-31 October

SAN DIEGO

#PSR25

WHO'S AFRAID OF AN AI AGENT?

A Panel Discussion on Navigating the Risks, Regulations, and Reality of Agentic AI.

WELCOME AND INTRODUCTIONS

Alesya Nasimova

AIGP, CIPP/E, CIPP/US, CIPM, Senior Director, Associate General Counsel, Privacy, Product and AI, Anaconda

Kate Parker

(Moderator)

President, Transcend

Laura Caroli

Senior Fellow, Wadhwani AI Center, Center for Strategic and International Studies

Do you know what an AI agent is?

1. Yes
2. No
3. I've heard of it,
   but not sure I could explain it

Do you know the fundamental differences between agentic AI and generative AI?

1. Yes
2. No
3. I have a general idea
   but could use more clarity

Has your company deployed AI agents into production?

1. Yes
2. No
3. In progress

Why This Conversation Matters

For Business Leaders: Agentic AI looks like efficiency.

For Privacy Leaders: Raises a whole new category of risk.

“The IT department of every company is going to be the HR department of AI agents in the future.”

- Jensen Huang, CEO, NVIDIA

What Are AI Agents?

The Economist

Weekly edition | The world in brief | War in the Middle East | War in Ukraine | United States | The world economy | Business | Artificial i

By Invitation | Trouble agents

AI agents are coming for your privacy, warns Meredith Whittaker

The Signal Foundation's president worries they will also blunt competition and undermine cyber-security

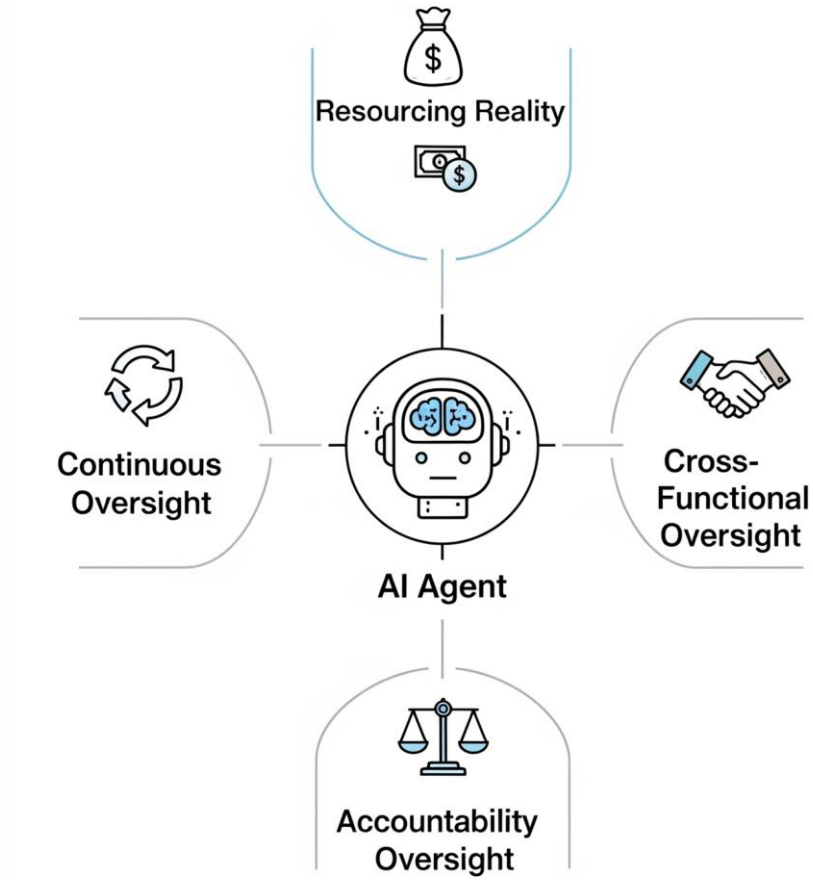
Share

#PSR25

Where AI Agents Create New Risks

When Agents Interact…

From Theory to Practice:
Managing Agentic Risks



“The time has come for us to formulate a vision of where we want AI to take us as a society and as humanity, and then we need to act and accelerate Europe in getting there."

Ursula von der Leyen, European Commission President

Where Do AI Agents Fit in the Law?

Where Do AI Agents Fit in the Law?

Region /Body	Key Focus	Implications
EU (AI Act)	**Risk-based approach;** obligations for General-Purpose AI (GPAI) and high-risk use cases (e.g., HR, finance).	**Uncertainty for agents:** Classification under the AI Act will determine compliance requirements.
U.S. (States)	**Patchwork regulation** focused on automated decision-making and algorithmic discrimination (e.g., Colorado AI Act, California ADMT rules).	**Fragmented obligations:** Organizations must navigate multiple, sometimes conflicting, state laws.
Global	**Voluntary standards** (e.g., ISO 42001, OECD AI Principles) for AI management and governance.	**Compliance is a moving target:** Organizations must anticipate conflicting regulations. ISO 42001 provides a framework for managing this complexity.

The Privacy Leader's Checklist

The Privacy Leader's Checklist

1. Clarify Your Agentic AI Footprint
2. Design for Explainability, Not Just Compliance
3. Embed Privacy in the Business Model
4. Stress Test for Regulatory Regimes
5. Control the Access Surface
6. Balance Innovation Moats with Guardrails
7. Communicate Strategically with Consumers, Investors, Regulators
8. Develop Instrument Metrics for Leadership

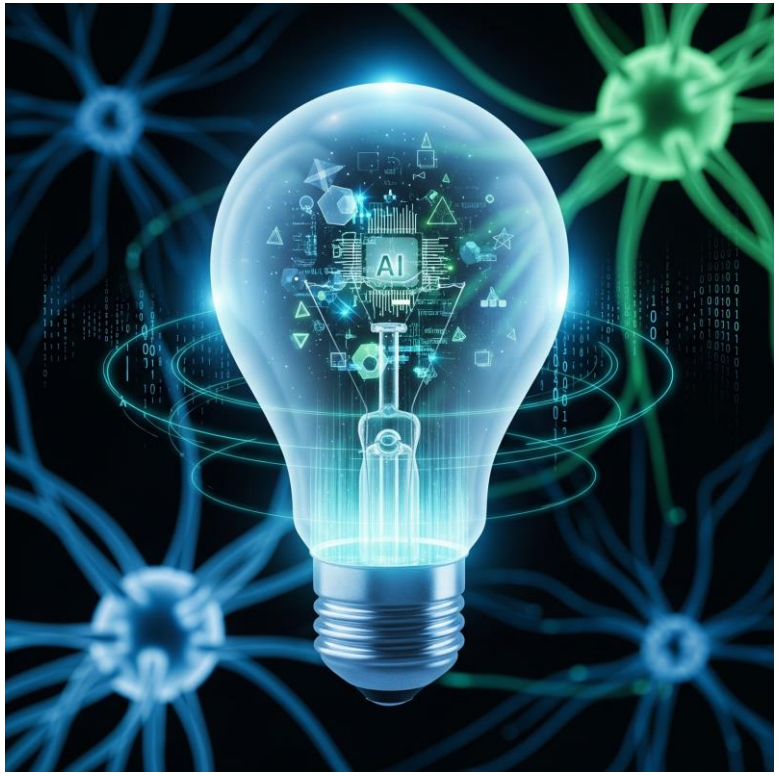
What do you see as the top risk of introducing agentic AI?

1. Loss of control
2. Data exposure
3. Regulatory exposure
4. PR and/or brand risk
5. Product safety risk

How do you feel about our agentic AI future?

1. Very excited
2. Cautiously hopeful
3. Neutral
4. Slightly worried
5. Really scared

One piece of advice for privacy leaders



Let’s continue the conversation online!

#PSR25

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!