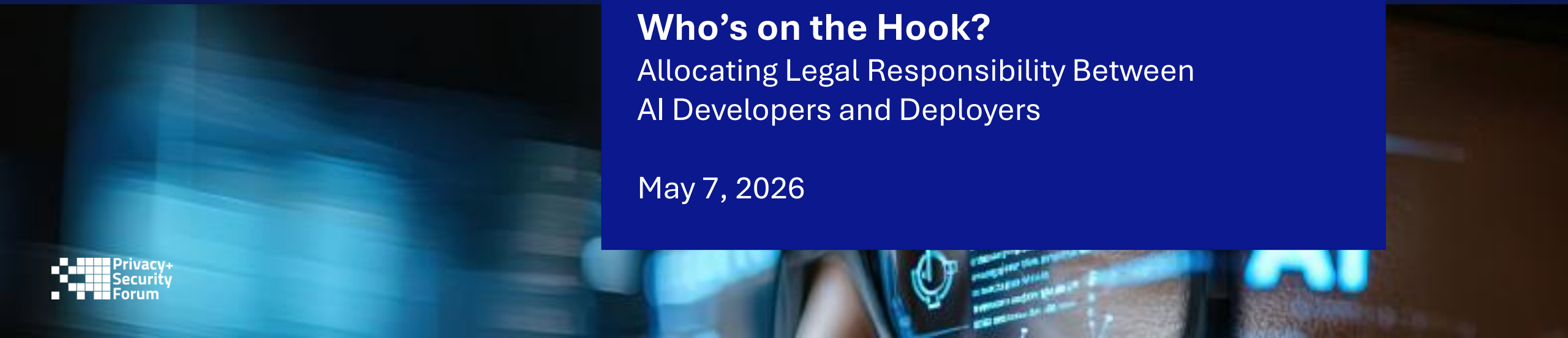
Privacy + Security Forum

Session:

Who's on the Hook?

Allocating Legal Responsibility Between AI Developers and Deployers

May 7, 2026



Privacy+ Security Forum

Speakers

Shelby Dolen
Associate
Troutman
Pepper Locke

Susan Fletcher
Chief Privacy Officer
Precisely

Laura Hamady
Partner
Troutman
Pepper Locke

Marlaina Pinto
Associate
Troutman
Pepper Locke

Privacy+ Security Forum

Overview

- Setting the Stage – Regulatory Landscape
- AI Use Cases
- Documentation and Impact Assessments
- Third-Party Risk Management
- Time to Negotiate – Who Holds the Risk?

Setting the Stage – Regulatory Landscape

Privacy+ Security Forum

State AI Governance Law – Comparison Chart

California	Colorado	New York	Utah	Texas
Assembly Bill 2013 Jan. 1, 2026 **Senate Bill 942** Jan. 1, 2026 **Senate Bill 53** Jan. 1, 2026	**Colorado AI Act**	**Responsible AI Safety and Education Act** January 1, 2027 ** To be amended per agreement with Governor*	**Utah AI Policy Act** May 1, 2024 **Senate Bill 226** May 7, 2025	**Texas Responsible Artificial Intelligence Governance Act** January 1, 2026

**Last updated April 28, 2026*

US Patchwork – States

High Risk / Consequential Decisions	AI or “automated decision tools” used for consequential decisions affecting people’s rights or access to critical services
Disclosures	Transparency: telling people when AI is being used and how
Chatbots	Disclose that a person is interacting with an automated system rather than a human
Pricing	Address algorithms that set or personalize prices
Employment	Regulate automated tools used in hiring, promotion, performance management, and termination
Health	Tools used in diagnosis, treatment recommendation, triage, telehealth, mental-health support, or health-plan decisions

US Patchwork – Federal

Congress hasn't passed a federal AI framework, but the EEOC, CFPB, FTC, and DOJ have all signaled they'll use existing authority to hold companies accountable for AI harms

Current administration's posture on AI regulation – National Policy Framework for Artificial Intelligence

EU AI Act – Provider vs. Deployer

Role	Description	Examples	Risks / Nuances / Pitfalls
Provider	• Develops an AI system (or has it developed) and places it on the market • May be located in the EU or places the system on the market in the EU	• AI vendors selling SaaS AI tools • Internal development team that builds an AI system and offers to clients • Cloud providers offering LLMs	• Provider status is based on who puts it on the market • Company that rebrands or modifies another's AI system can still be a provider • Anticipate potential misuse
Deployer	• Uses an AI system	• Employers using AI for hiring • Hospitals using AI for diagnostics	• Can shift into a provider if the deployer uses the AI system beyond its intended purposes

EU AI Act – Risk Categories

Prohibited	High-Risk	General Purpose AI Models	General Purpose AI Models w/ Systemic Risks	Transparency
• Social behavioral scoring • Emotion-recognition at work and in education • Exploit people's vulnerabilities • Behavioral manipulation and circumvention of free will • Untargeted scraping of facial images for recognition • Biometric categorization systems that use certain sensitive characteristics • Predictive policing	Pose a significant risk to health, safety or fundamental rights, including in the following categories: • Profiling • Medical devices • Vehicles • Emotion-recognition systems • Law enforcement • Credit scoring	Display significant generality, are capable of competently performing a wide range of distinct tasks, regardless of how they are placed on the market, and can be integrated into a variety of downstream systems or applications.	General-purpose AI models that have "high-impact capabilities" that match or exceed the capabilities recorded in the most advanced general-purpose AI models	Specific transparency obligations are imposed on providers and deployers of certain AI systems

EU AI Act – Compliance Dates

Feb. 2, 2025

Prohibitions on unacceptable risk AI

Aug. 2, 2025

Obligations for general-purpose AI governance

Aug. 2, 2026

All rules of the AI Act become applicable, including obligations for high-risk systems

Aug. 2, 2027

Obligations for all other high-risk systems

AI Use Cases

Privacy+ Security Forum

AI Tracks

Internal Use

Threshold Assessments

Vendor Questionnaire

Impact Assessments

Contract Negotiations

Implementation

Develop / Deploy

Purpose / Use Case

Testing

Impact Assessments

Develop Contract Terms

Market / Deploy

Third Party Risk Management

Privacy+ Security Forum

Due Diligence – Threshold Assessment

Risk Rating	Principals Associated Risk Rating / Potential Harms	Next Steps / Required Information	Required Contract Terms	Required Non-Contract Risk Mitigations / Controls
Unacceptable Risk	No additional review by the AI task force/committee is needed as requests that fall into the Unacceptable Risk use case will not be approved.	• Conduct applicable assessments • Send vendor questionnaire • Provide list of follow up questions to vendor	• Indemnity • Liability • Reps/Warranties • Ownership of data • Training of model	• Testing • Security controls
High Risk	Secondary review by AI task force/committee is necessary to assess and determine what risk mitigants and controls are necessary for approval	• Conduct applicable assessments • Send vendor questionnaire • Provide list of follow up questions to vendor	• Indemnity • Liability • Reps/Warranties • Ownership of data • Training of model	• Testing • Security controls
Limited Risk	Secondary review by AI task force/committee is necessary to assess and determine what risk mitigants and controls are necessary for approval	• Determine whether approved tool • Conduct applicable assessments	• Reps/Warranties • Ownership of data • Training of model	• Testing • Security controls
Low Risk	No additional review by AI task force/committee is needed	• Determine whether approved tool	• Ownership of data • Training of model	• Security controls

Documentation and Impact Assessments

Privacy+ Security Forum

Documentation Considerations

EU AI Act Documentation Requirements

- Conformity Assessments
- Fundamental Rights Impact Assessment (High-Risk)

CO AI Act Documentation Requirements*

- Impact Assessments (Deployer)
- Publicly Available Statement (Developer / Deployer)

Impact Assessments

- Consider other assessment requirements under data protection laws
- CCPA Regulations – Risk Assessments for ADMT

**Last updated April 28, 2026*

Time to Negotiate – Who Holds the Risk?

Privacy+ Security Forum

Key Contractual Terms

- Indemnity and liability gaps
- Liability limits
- AI-specific harms
- Representations / warranties
- Ownership of data

AI Terms – Examples

Representations / Warranties

- All necessary rights, notices, and consents to provide the AI, including any third-party models / tools and training data
- IP infringement, misappropriation, violation
- Breach of individual privacy rights
- No complaint, litigation, claim, or proceeding regarding the AI or training data

Indemnity

- IP infringement, misappropriation, violation
- Breach of confidentiality
- Breach of data protection / data breach

Ownership

- Ownership of input vs. output

Stay in touch: Continue the conversation with us

Shelby Dolen
linkedin.com/in/shelby-dolen/

Susan Fletcher
linkedin.com/in/susan-ndongwa-fletcher/

Laura Hamady
linkedin.com/in/laurahamady/

Marlaina Pinto
linkedin.com/in/marlainazpinto/

Privacy+ Security Forum

Troutman Pepper Locke Resources

Privacy + Cyber + AI Blog

US State Data Privacy and AI Laws

State Artificial Intelligence Law Tracker

Privacy+ Security Forum