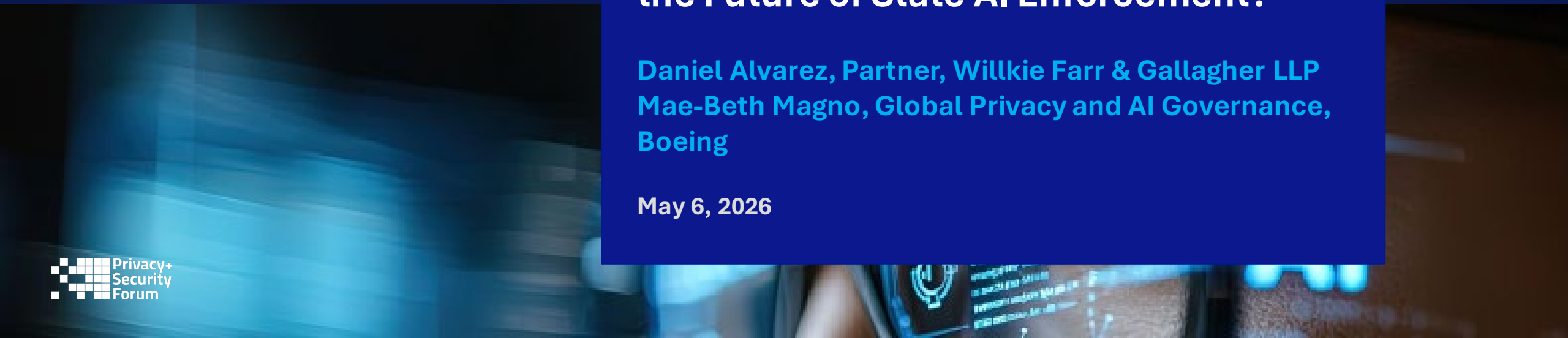
Privacy + Security Forum

Sound and Fury? What Can State Privacy Enforcement Teach Us About the Future of State AI Enforcement?

Daniel Alvarez, Partner, Willkie Farr & Gallagher LLP
Mae-Beth Magno, Global Privacy and AI Governance, Boeing

May 6, 2026



Privacy+ Security Forum

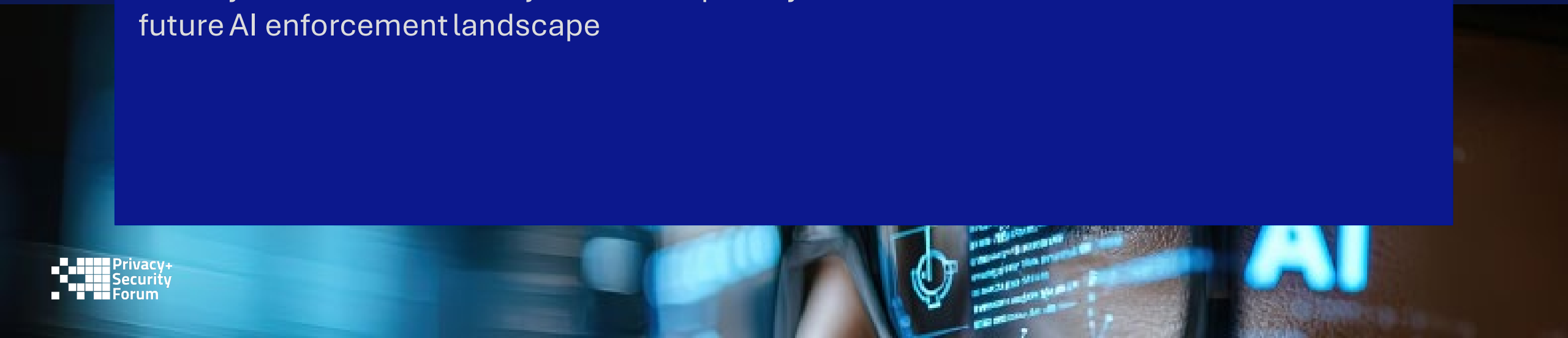
Session: Privacy Enforcement Trends and AI Compliance

Setting the Stage

- Privacy enforcement in the U.S. has expanded dramatically — from traditional data-breach actions into algorithmic accountability, sensitive data, and automated decision-making

- These enforcement developments now serve as the foundation for emerging AI compliance expectations

- Today's Goal: Examine major trends in privacy enforcement and draw lessons for the future AI enforcement landscape



Privacy+ Security Forum

Development 1: An AI Wild West?

The FTC Act and Consumer Protection Laws Step Into the Breach

- Common misperception: "The U.S. has no AI law"
- FTC Act (Section 5) and state counterparts provide a baseline legal framework for data collection activities
- FTC and state AGs built a significant "privacy common law" over decades
- SEC cybersecurity disclosure rules extend regulatory authority
- Bottom line: Laws are in place and must be observed at the risk of significant enforcement penalties

Recent Enforcement Examples

FTC v. Kochava (2022–2024)

- Sued data broker for selling geolocation data enabling tracking of visits to sensitive locations (reproductive health clinics, places of worship); relied on Section 5 unfairness authority

FTC v. Rite Aid (2023)

- Challenged facial recognition with disproportionate false positives affecting minorities; framed as Section 5 unfair practice causing substantial consumer injury

SEC Cybersecurity Rules (2023)

- Required disclosure of material cybersecurity incidents within 4 business days; annual cybersecurity risk management disclosures

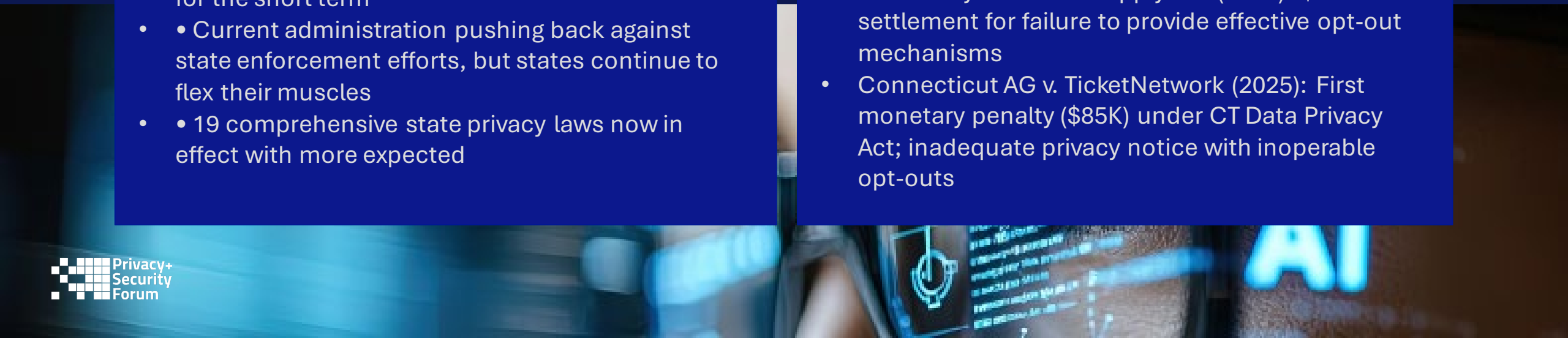
Development 2: State Enforcement Takes Center Stage

Key Developments

- As federal enforcement priorities shift with changing administrations, state AGs and state privacy agencies have stepped into the enforcement role
- Coordinated multi-state enforcement activity increasingly common — even in the "reddest" states
- State enforcement is likely the new center of gravity for the short term
- • Current administration pushing back against state enforcement efforts, but states continue to flex their muscles
- • 19 comprehensive state privacy laws now in effect with more expected

Key Enforcement Examples

- Texas AG — $1.4 Billion Biometric Data Settlement (2025): One of the largest data privacy settlements ever reached by a single state
- Texas AG v. Allstate/Arity (2025): First-ever privacy lawsuit under a state comprehensive privacy law; unlawful collection of geolocation data from 45M+ Americans
- CalPrivacy v. Tractor Supply Co. (2025): $1.35M settlement for failure to provide effective opt-out mechanisms
- Connecticut AG v. TicketNetwork (2025): First monetary penalty ($85K) under CT Data Privacy Act; inadequate privacy notice with inoperable opt-outs



Privacy+ Security Forum

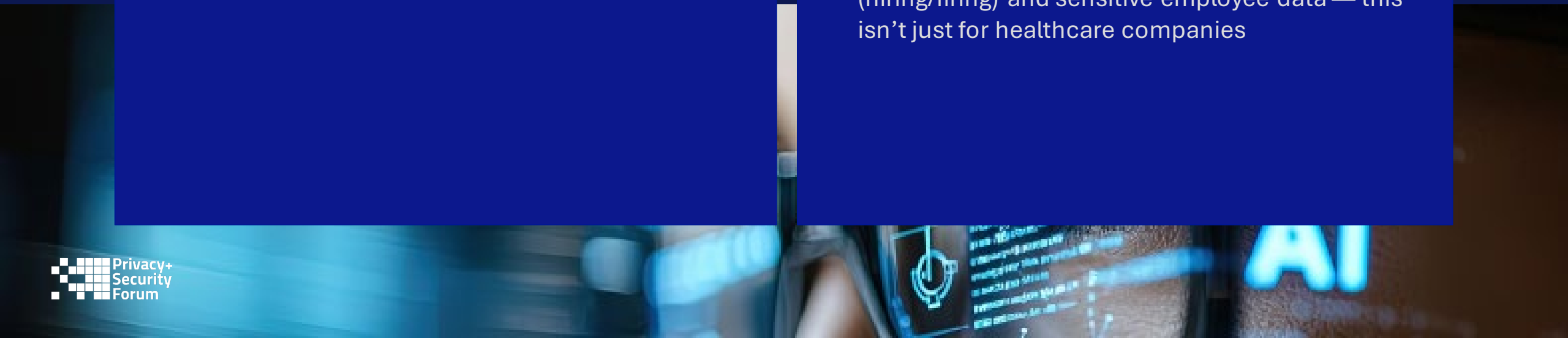
Development 3: Sensitive Data = High-Risk Use Cases

The Sensitive Data Paradigm

- FTC's 2012 Privacy Report: Protections should be a function of data sensitivity — now a core concept in GDPR, CCPA, and state laws
- Since 2022, aggressive enforcement around sensitive data categories, especially health data
- FTC's Health Breach Notification Rule revived as a powerful enforcement tool

Key Cases and Implications

- Risk-based approach now bleeding into AI-specific rules (EU AI Act, Colorado AI Law)
- Key cases:
  - GoodRx ($1.5M)
  - BetterHelp ($7.8M)
  - CA AG v. Healthline ($1.55M — largest CCPA settlement)
- Every company handles "high-risk" activities (hiring/firing) and sensitive employee data — this isn't just for healthcare companies



Privacy+ Security Forum

Development 4: Global Enforcement

European Regulators Leverage GDPR

- European data protection authorities directly targeting AI systems under GDPR — creating precedent that may be useful examples for U.S. regulators
- Italy v. OpenAI/ChatGPT (2024): €15M fine — first generative AI-related fine under GDPR
- Italy v. Luka/Replika (2025): €5M fine for AI chatbot privacy violations

Global Enforcement Landscape

- Clearview AI: Fines across Italy, France, UK, Netherlands, Greece; Dutch authority imposed €30.5M fine
- EDPB task force coordinating oversight of generative AI; Irish DPC paused Meta's AI training plans
- EU Digital Omnibus Proposals (Nov. 2025): Potential regulatory relaxation alongside continued enforcement?

Privacy+ Security Forum

Development 5: Don’t Forget the Plaintiff’s Bar

Private Litigation Can Drive Enforcement

- Private plaintiffs push novel theories based on existing laws; advocate for private rights of action in new laws
- CIPA "Session Replay" and Chatbot Litigation (2023–present): Class actions alleging wiretapping by session replay tools and AI chatbots
- BIPA Class Actions: $650M Facebook settlement; $228M BNSF Railway verdict; statutory damages $1K–$5K per violation
- VPPA Litigation: Decades-old statute invoked against modern tracking technologies

Emerging Litigation Trends

- AI Training Data Class Actions: Suits against OpenAI, Meta, Google, Stability AI for training on copyrighted/personal data
- Key risk: Creative legal theories leverage narrow statutes against modern AI practices

Privacy+ Security Forum

Development 6: Algorithmic Disgorgement

The FTC's Novel AI-Era Remedy

- Since 2019, FTC requires deletion of not only improperly collected data but also algorithms, models, and work product derived from it
- Principle: "Companies should not profit from illegally collected data or any algorithm developed using it"
- Key cases: Cambridge Analytica (2019), Everalbum/Paravision (2021), WW International/Kurbo (2022), Ring (2023), Rite Aid (2023)

Risk Assessment

- Current administration signaling pullback (Rytr LLC consent order set aside, Dec. 2025), but precedent remains
- Critical risk: Puts the AI model itself — often a company's most valuable asset — at risk
- Vendor implications: Disgorgement orders can cascade through third-party AI procurement relationships

Privacy+ Security Forum

Critical Questions: For Compliance Leaders

Educating Stakeholders
How do you educate stakeholders that existing laws already regulate AI?

Multi-State Compliance
How do you build compliance programs for a multi-state patchwork that increasingly includes AI-specific requirements?

Evolving Regulations
How do you stay on top of rapidly evolving state and international regulations?

Data Governance
What governance measures address data sourcing and provenance for AI training data?

Risk Calculus
How should the risk calculus differ when facing regulators vs. private plaintiffs?

Unified Compliance
How do you approach unified vs. jurisdiction-by-jurisdiction compliance (lessons from privacy for AI)?

Privacy + Security Forum

Key Takeaways: Enforcement Trends and AI Compliance

Five Key Takeaways

1. Privacy enforcement precedent directly informs AI compliance expectations — even without comprehensive federal AI legislation
2. State enforcement is the new center of gravity — 19 comprehensive state privacy laws, bipartisan enforcement consortium, and California's ADMT regulations now in effect
3. Sensitive data and "high-risk" activities are the enforcement frontier — AI systems processing health, biometric, and geolocation data face highest regulatory risk
4. Global enforcement (especially EU) is creating compliance expectations U.S. companies cannot ignore — GDPR became the blueprint for CCPA; EU AI enforcement may follow the same course
5. The political landscape is dynamic — building compliance infrastructure now is the most defensible approach regardless of the political cycle

Privacy+ Security Forum

Your Presenters

Daniel K Alvarez
Partner
Willkie Farr & Gallagher LLP

Mae-Beth Magno
Global Privacy and AI Governance
Boeing

THANK YOU!

Privacy+ Security Forum