AI Regulation Is Here: What Businesses Need to Know Now About Risk, Compliance, and Governance

By: Jason T. Seay, AIGP, CIPP-US

July 1, 2026

Artificial intelligence is rapidly transforming how companies operate, but with that transformation comes increasing legal scrutiny, regulatory complexity, and operational risk. AI is no longer an emerging issue—it is a current business and legal priority.

Here are seven key takeaways from my presentation at the BSidesOK AI Security Summit.

1. AI Risk Is Broad, Immediate, and Business-Critical

Organizations must evaluate AI beyond technical performance, focusing on legal, reputational, and operational consequences.

- AI-related harms can include:
    - Reputational damage
    - Regulatory exposure
    - Discrimination and bias risks
    - Data privacy violations
    - Economic and societal impacts
- AI amplifies existing risks due to its scale, speed, and automation capabilities

Why does it matter?
Failure to proactively identify and mitigate these risks can lead to enforcement actions, litigation, and brand damage—often before issues are fully understood.

2. There Is No Single AI Law, But Significant Legal Exposure Exists

In the U.S., AI is governed through a patchwork of existing laws and emerging state regulations, not a single comprehensive statute.

- Existing laws already apply, including:
    - Consumer protection (e.g., misleading AI claims)

- Anti-discrimination laws (e.g., hiring, lending)
- Privacy and data governance laws

- Regulators such as the FTC are actively taking enforcement action for AI-related misconduct

Why does it matter?
Companies cannot assume they are "unregulated" simply because there is no omnibus AI law. Legal exposure already exists across multiple fronts.

3. State-Level AI Regulation Is Accelerating Quickly

Several states have already enacted AI-specific laws with immediate and near-term compliance obligations:

- **California (2026):**
  - AI transparency requirements for training data
  - Disclosure obligations for chatbots and synthetic content
- **Colorado (2026):**
  - Anti-discrimination and reporting requirements for high-risk AI (subject to change under new legislation currently under consideration in Colorado; see SB 26-189)
- **Texas (2026):**
  - Comprehensive AI governance framework and regulatory sandbox
- **New York & Illinois (2026):**
  - Reporting, safety, and civil rights implications for AI systems

Why does it matter?
Businesses operating across multiple jurisdictions must manage inconsistent and evolving compliance obligations, increasing operational complexity and risk.

4. Your Role in the AI Ecosystem Determines Your Liability

Regulatory frameworks increasingly distinguish between different participants in the AI lifecycle, such as:

- **Providers:** Design and develop AI systems (highest regulatory burden)
- **Deployers:** Use AI within business operations (compliance and oversight obligations)
- **Importers/Distributors:** Ensure systems meet regulatory requirements before market entry

Why does it matter?
Understanding your role is critical. Liability and compliance obligations vary significantly depending on how your business interacts with AI.

5. AI Governance Must Span the Entire Lifecycle

Effective AI governance is not a one-time exercise; it must be embedded across the full AI tool lifecycle:

- Planning and problem definition
- Data collection and bias mitigation
- Model development and documentation
- Testing for fairness and accuracy
- Deployment with oversight and reporting
- Ongoing monitoring and maintenance
- Proper decommissioning and data handling

Why does it matter?
Regulators and stakeholders increasingly expect "governance by design," not retroactive fixes after deployment.

6. Risk-Based Frameworks Are Becoming the Global Standard

Most regulatory approaches categorize AI systems by risk level, such as:

- **Prohibited:** Banned uses (e.g., certain biometric surveillance)
- **High Risk:** Subject to strict oversight and documentation
- **Limited Risk:** Transparency and disclosure requirements
- **Minimal Risk:** Voluntary standards

Why does it matter?
Companies must assess where their AI tools fall within these categories to determine compliance obligations and acceptable use cases.

7. Data, Cybersecurity, and Liability Are Emerging Pressure Points

Key trends shaping AI-related risk include:

- **Data quality and bias:** AI outputs are only as reliable as training data
- **Cybersecurity and confidentiality:** Increased threat exposure through the use of AI systems
- **Product liability questions:** Whether AI systems will be treated as "products" under existing product liability laws
- **Internal governance gaps:** Lack of policies, training, and oversight structures

Why does it matter?
These issues are likely to drive the next wave of enforcement and litigation, particularly for companies deploying AI at scale.

What Businesses Should Do Now

To stay ahead of regulatory and operational risk, organizations should:

- **Conduct an AI risk assessment** across all business functions
- **Map AI use cases** to applicable laws and regulatory frameworks
- **Implement governance policies** covering development, deployment, and monitoring of AI tools
- **Establish internal accountability** (legal, compliance, IT, and business stakeholders)
- **Audit data sources and outputs** for bias, accuracy, and compliance
- **Prepare for disclosures and transparency requirements**

AI presents significant opportunities, but also heightened legal, regulatory, and reputational risk. Organizations that take a proactive, structured approach to AI governance will be best positioned to innovate confidently while minimizing exposure.

This Alert was prepared by Jason Seay, AIGP, CIPP-US, a member of GableGotwals' Cybersecurity and Data Privacy Team. For more information, please contact Jason or a member of the team.

Jason T. Seay, AIGP, CIPP-US

918-595-4832

jseay@gablelaw.com