ROPES & GRAY

AI and the Data Protection Landscape

May 2026

Welcome and Introductions

Edward McNicholas, JD

Partner and Practice Group Leader

Data, Privacy & Cybersecurity Practice

Ropes & Gray LLP

Fran Faircloth, JD

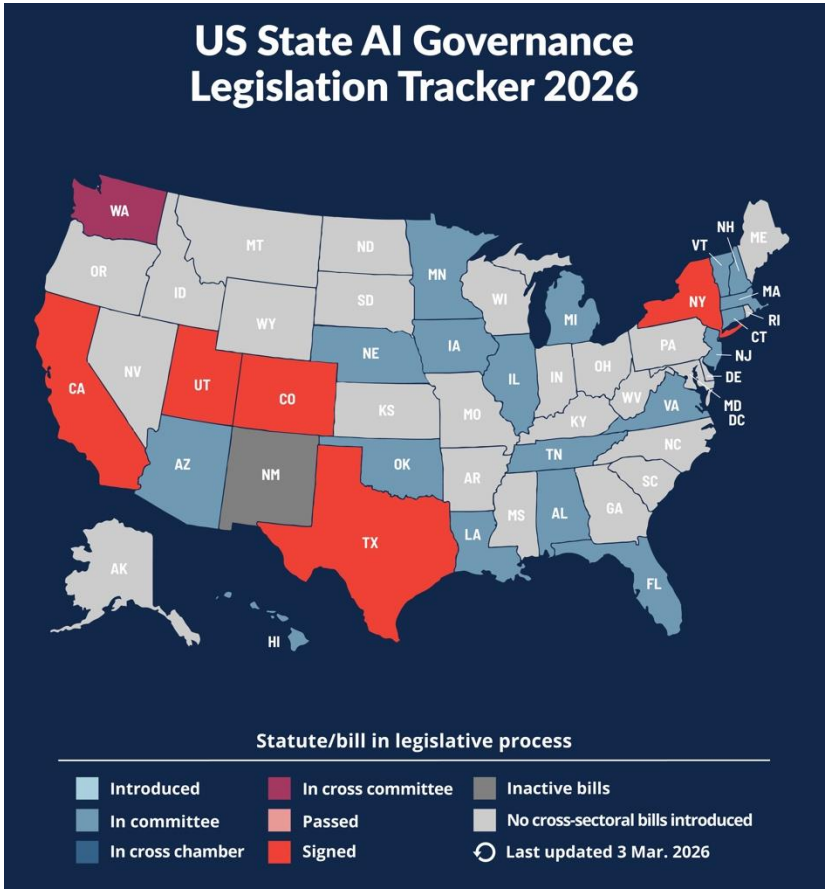
Partner

Data, Privacy & Cybersecurity Practice

Ropes & Gray LLP

AI Legal & Regulatory Backdrop

- **In the US**, there is no global or federal statute governing AI
- Various states and federal agencies regulate:
  - **States with broad AI governance regulations:** California, Colorado, Texas, New York, Utah
  - **Federal agencies:** DOJ, FTC, SEC, CFTC
  - Various other states and cities have laws regulating or impacting AI use in specific contexts, including health care
- **In the European Union**, the **"EU AI Act"** provides guidance on risks and risk mitigation, classifying AI according to risk levels, and primarily focusing on developers of "high risk" AI

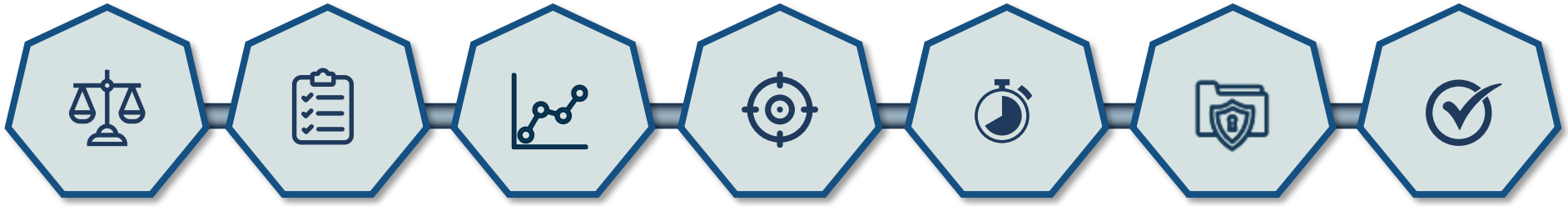


Credit: International Association of Privacy Professionals (IAPP)

Privacy and Data Protection Principles

ROPES & GRAY

Article 5 of GDPR discusses seven key principles related to the processing of personal data



Transparency, Fairness & Lawfulness

Personal data should be processed lawfully, fairly and in a manner that is transparent to the data subject.

Purpose Limitation

Personal data should be collected for specified, explicit and legitimate purposes.

Data Minimization

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

Personal data should be accurate and, where necessary, kept up to date.

Personal data that are inaccurate should be promptly erased or rectified.

Storage Limitation

Personal data should be kept for no longer than is necessary for the purposes for which the personal data are processed.

Integrity & Confidentiality

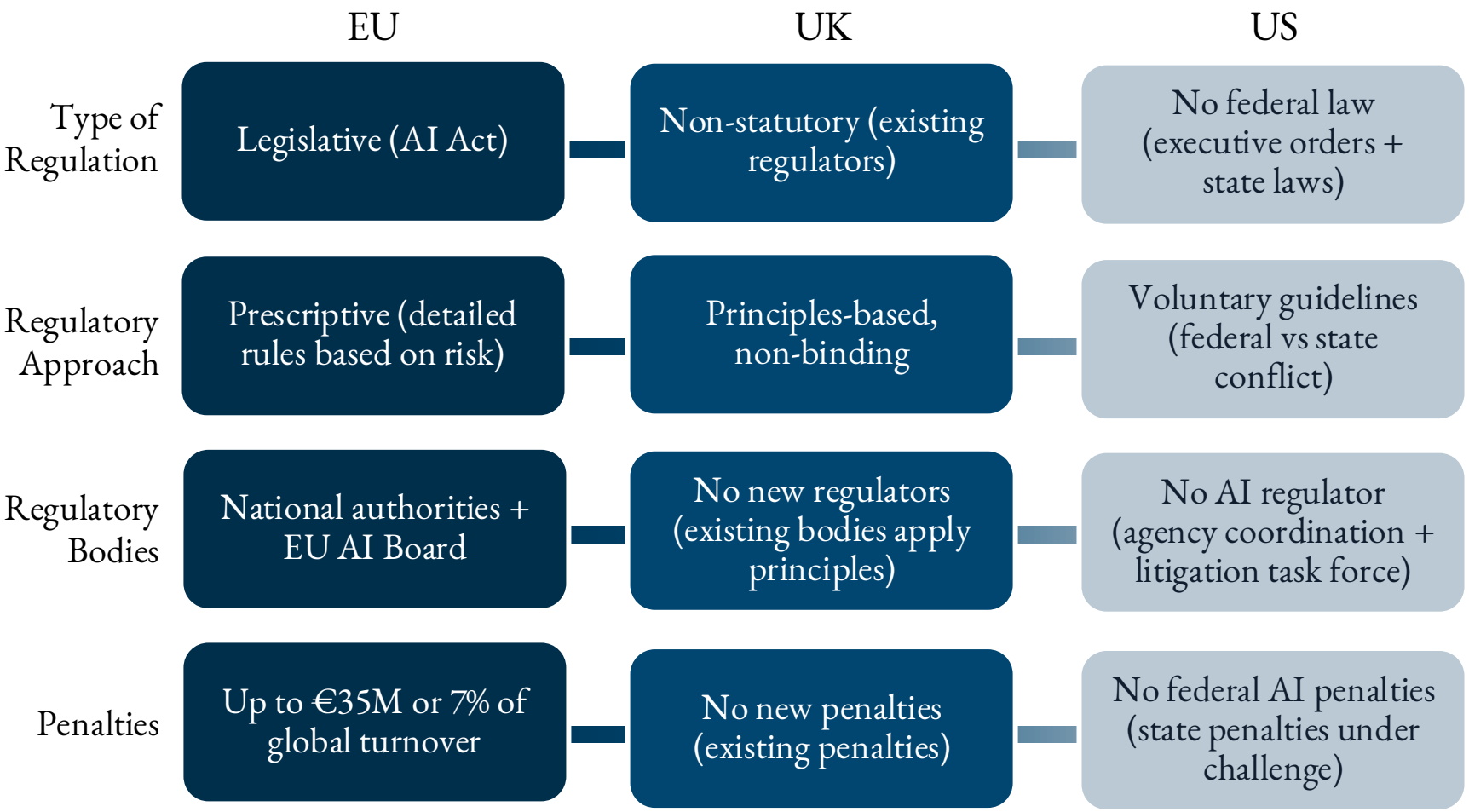
Personal data must be processed securely, with appropriate technical and organisational measures to prevent unauthorized or unlawful processing and accidental loss or damage.

Accountability

Ongoing recordkeeping and documentation of policies and practices, compliance with measures that give effect to these principles.

AI Legal & Regulatory Backdrop

ROPES & GRAY



AI Legal & Regulatory Backdrop

ROPES & GRAY

- **Businesses and organizations can also look to the following voluntary frameworks that provide guidance on AI risk management and accountability:**
  - ✓ National Institute of Standards and Technology's (NIST) AI Risk Management Framework
    - NIST's Framework is intended to help "incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems" and recommends four broad categories of risk management ("govern," "map," "measure," and "manage").
  - ✓ Government Accountability Office's (GAO) AI Accountability Framework
    - This framework was developed to help managers "ensure accountability and responsible use of artificial intelligence (AI) in government programs and processes" and focuses on "governance, data, performance, and monitoring," and includes questions for consideration for entities using AI systems.
  - ✓ Organisation for Economic Co-operation and Development's (OECD) Principles on Artificial Intelligence
    - These Principles are meant to "guide AI actors in their efforts to develop trustworthy AI and provide policymakers with recommendations for effective AI policies." Principles include transparency and explainability, accountability, security and safety, and fairness and privacy. Other countries use these Principles to "shape policies and create AI risk frameworks."
- **Some of these various frameworks and principles can potentially help guide AI users and developers in their own adoption and implementation of AI.**

Global AI Regulation: The UK and EU

UK Approach to AI Regulation

- Technologically neutral approach, with a focus on context and sector-specific application.
- Targeted rules for high-risk AI applications (particularly generative AI and deepfakes) through existing legislation.
- AI Bill proposed for late 2026 covering frontier models, copyright issues, and possibly establish a statutory AI authority – but no firm legislation has been set, and further delays are expected.
- Until then, UK operates under five cross-sector principles: safety, transparency, fairness, accountability, and contestability

EU AI Act

- First attempt at a legislative framework for AI
- Classifies AI according to risk, with outright bans for AI that presents the highest risk.
- Imposes significant obligations on a range of parties involved with high-risk AI systems.
- Broad territorial scope with an extraterritorial effect, covering providers and users of AI systems within and outside the E.U.
- Enforcement options include fines of up to EUR 35 million or 7% of global revenue, as well as requests for information and powers to compel corrective measures or to recall the AI system from the market.

Global AI Regulation: The EU AI Act

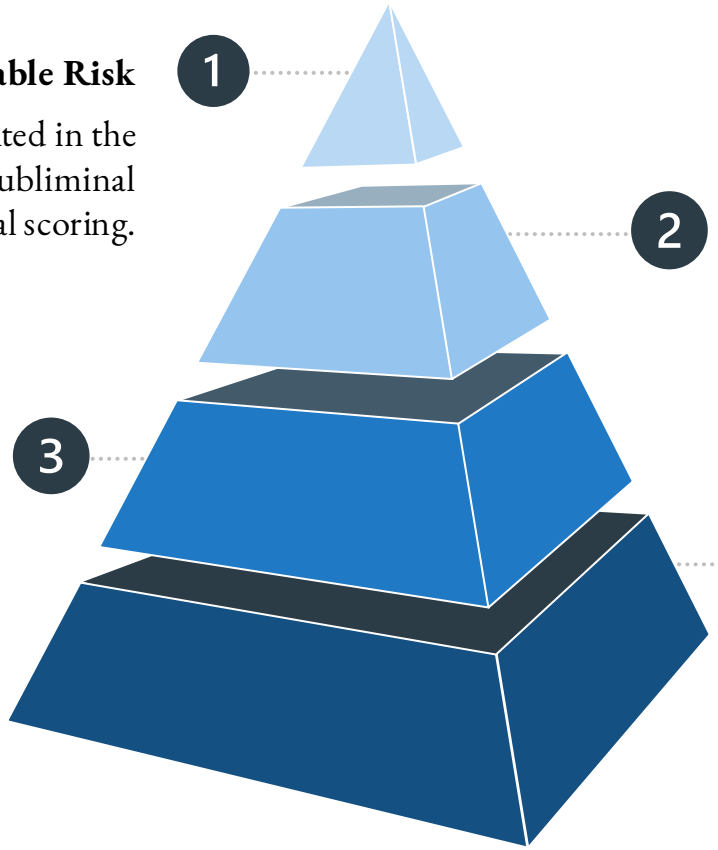
ROPES & GRAY

Unacceptable Risk

Highest level of risk prohibited in the EU, e.g., AI systems using subliminal manipulation or general social scoring.

Limited Risk

Includes AI systems with a risk or manipulation or deceit, e.g., chatbots or emotion recognition systems. Humans must be informed about their interaction with the AI.



High Risk

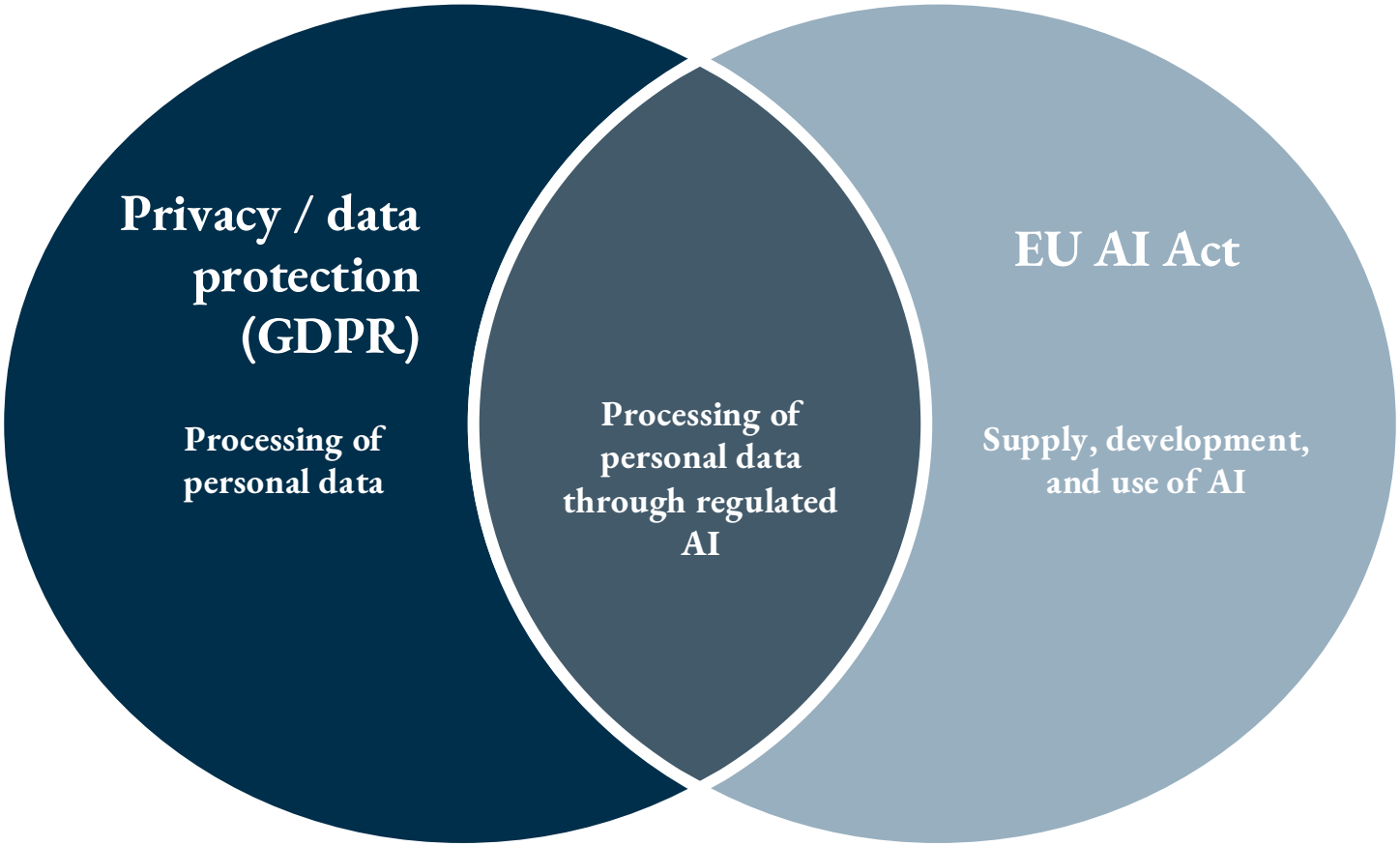
Most regulated AI systems, as these have the potential to cause significant harm if they fail or are misused, e.g., if used in law enforcement or recruiting.

Minimal Risk

All other AI systems, e.g., a spam filter, which can be deployed without additional restrictions.

As well as intended use, the Act allows the Commission to consider the **"extent to which the AI system acts autonomously"** when assessing whether a system results in an adverse impact on fundamental rights.

Global AI Regulation: The UK and EU



While the EU AI Act focuses primarily on the **technical security and risk classification** of systems, the GDPR still sets the framework for processing of personal data and managing data subject rights.

Key Developments at the Federal Level

ROPES & GRAY

Administration Approach

Significant shifts in norms in the second Trump Administration continue to impact governance of AI and its impact on data protection

- Restructuring of civil service generally
  - Democratic **FTC** Commissioners fired
  - Privacy & Civil Liberties Oversight Board firings
  - **CISA** staff cut / mission uncertain
  - Bulk personal data transfers to China restricted

- Shift away from multilateral engagement.

Key Developments at the Federal Level

- ***January 2025*** – President Trump revoked President Biden's Executive Order on AI and issued Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence," assigning select advisers to develop an "action plan" to "sustain and enhance America's global AI dominance."
- ***July 2025*** – The Trump Administration released its federal action plan to promote AI innovation and deregulation across industries, including healthcare, and directed agencies to identify and roll back federal regulations that may impede AI development.
- ***December 2025*** – The Trump Administration issued an Executive Order establishing a national AI policy framework, aimed at preempting state AI regulations and promoting AI innovation. The order establishes a task force to challenge state laws, instructs the Secretary of Commerce to refer onerous state AI laws for scrutiny, and tasks federal agencies with considering preemptive reporting and disclosure. It also imposes restrictions on federal funding for states with conflicting AI laws and calls for legislation to preempt state regulation, with exceptions for child safety and certain state functions.
- ***March 2026*** – The Trump Administration issued a National AI Legislative Framework urging Congress to develop federal legislation around six objectives, including privacy rights of minors; construction of data centers; intellectual property; free speech; innovation; and education and job training.

Key Developments at the Federal Level

President Trump's "Cyber Strategy for America," released March 6, 2026

- "We will deploy the full suite of U.S. government defensive **and offensive** cyber operations. We will **unleash the private sector by creating incentives to identify and disrupt adversary networks** and scale our national capabilities."
- "We will work to adopt **AI-powered cybersecurity solutions** to defend federal networks and deter intrusions at scale."
- "And we will secure the AI technology stack—including our data centers—and promote innovation in AI security. We will swiftly implement AI-enabled cyber tools to detect, divert, and deceive threat actors."
- "We will **rapidly adopt and promote agentic AI** in ways that securely scale network defense and disruption."
- "Through **cyber diplomacy**, we will ensure that AI—particularly generative AI and agentic AI—advances innovation and global stability. We will secure the data, infrastructure, and models that underpin U.S. leadership in AI and we will call out and **frustrate the spread of foreign AI platforms that censor, surveil, and mislead** their users."

State AI Regulation: Health Care Sector

Given the absence of federal legislation, states are increasingly proposing and enacting legislation impacting use of AI in health care, particularly focusing on health tech developers of AI and payors, providers, and their vendors deploying AI in health care contexts

For health care providers, state laws focus on:

- Use of AI in treatment / provision of health care
- Processing of sensitive information (e.g., mental health, substance abuse, reproductive health)
- Use of AI in patient communications, such as chatbots

State laws are increasingly imposing compliance and transparency requirements for health care stakeholders using AI, particularly:

- Implementing and maintaining AI compliance programs (policies, procedures, training)
- Risk / impact assessments, monitoring, or auditing
- Ensuring public transparency/disclosure to users
- Submission or inspection by state regulatory body

State AI Regulation: Colorado AI Act

Colorado Senate Bill 24-205: Enacted in May 2024

- **Regulates "High-Risk" AI systems:** Systems that make a consequential decisions related to sensitive areas such as employment or insurance.
- **Regulates algorithmic discrimination and prohibits disparate treatment by AI.**
- **Required disclosures:** Statement from companies who use or develop High-Risk systems regarding the intended use cases and benefits of AI, analysis of risk, description of data inputted into the AI, post-deployment safeguards, and other required disclosures.
    - Transparency: even non-High-Risk AI systems must disclose AI use to consumers.
    - Incident reporting obligations.
- **AI deployment obligations:** entities that use AI from third parties must have robust disclosure and compliance programs.
- Encouraged by Colorado, other states like CA, CT, NY, TX, and UT have also enacted bills targeting AI governance, transparency, and responsibility.

State AI Regulation: NY AI Bot Bill

ROPES & GRAY

NY Proposed Bill SB 7263: AI Chatbot Liability

- **What it does:** Imposes civil liability on "proprietors" of AI chatbots that provide responses constituting the unauthorized practice of a licensed profession (e.g., law, medicine) under NY Education Law or Judiciary Law
- **Who is liable:** "Proprietors" means entities that own, operate or deploy the chatbot. Third-party developers who merely license their technology are expressly excluded.
- **Disclosure required:** Proprietors must provide clear, conspicuous notice that users are interacting with an AI chatbot – but disclosure alone is not a defense to liability.
- **Private right of action:** Individuals may sue to recover actual damages; willful violations also trigger attorneys' fees.
- **Carve-outs:** Does not prohibit general Q&A use of chatbots or prevent licensed professionals from using AI in their work.
- **Status:** Passed NY Senate's Internet & Technology Committee; currently on the NY Senate Floor Calendar.
- **Key open question:** How courts will interpret what constitutes a "substantive" response amounting to professional practice – and the resulting exposure for chatbot deployers.

Key Regulatory Issues

ROPES & GRAY

Risk Classification under EU AI Act	Transparency and Explainability	Human Oversight	Accountability	Individual Data Rights
Many common AI uses (hiring, credit scoring, fraud detection) – may fall within the high-risk category of the EU AI Act, triggering strict compliance duties.	AI makes transparency difficult; its decision paths are complex and changing, making it harder to provide clear and meaningful explanations.	AI (and agentic AI) complicates oversight requirements: these systems are designed to reduce human involvement. The task of balancing the right level of human involvement with the increased autonomy of these models will be a key challenge for early adopters of AI.	AI systems involve multiple actors—model providers, system providers, and deployers—each with different expertise, resources, and information. Diffusion of responsibility makes it difficult to assign clear accountability for risk management and compliance.	Responding to data rights requests can be especially difficult with AI, given its use of memory, logs, and complex decision paths.

Implementing AI Policies

ROPES & GRAY

- **Develop and implement an internal AI policy or framework that includes:**
  - Overall governance responsibilities, including mechanisms for oversight
  - Data privacy provisions
    - *Outline how data will be collected, stored, used, and managed to ensure compliance with data privacy laws*
  - Safeguards for intellectual property and sensitive / confidential information
  - Approved AI tools and appropriate use practices by employees and third-parties on the Company's behalf
  - Best practices for employees' use of sanctioned AI
    - *Outline what employees can use to train the AI, and when its use should be disclosed to managers or clients*
  - Clear guidelines on transparency and accountability
  - Appoint a supervisory role (could be a CTO or a newly created position) that oversees compliance with policy and regularly reports to senior management/the Board
- **Develop and use measures to address potential discrimination / bias through the use of AI tools and consider adopting ethical principles.**

AI Governance: Confidentiality & Security

ROPES & GRAY

- **Training AI models requires substantial input of data, making AI platforms and their training systems potentially prime targets by criminal actors.**
- **Data inputted into public AI systems (e.g., PII, PHI, trade secrets) can be reused for additional training, potentially inadvertently exposing sensitive data to public sources.**
  - In recognition of this possibility, some courts have issued standing orders and local rules requiring parties to take precautions when using AI tools due to concerns of possible breaches of confidentiality and privilege. See, e.g., Standing Order of Magistrate Judge Peter H. Kang (N.D. Cal.).
  - In 2023, OpenAI admitted to a bug which allowed users to see the titles of other users' conversation history.

BUSINESS INSIDER

Subscribe | Newsletters

TECH

OpenAI quickly rolled back a new feature that allowed users to make private conversations with ChatGPT searchable

By Katherine Tangalakis-Lippert and Henry Chandonnet

- ChatGPT also removed a new feature which allowed users to make their private ChatGPT conversations discoverable by search engines, citing privacy and security concerns.
- Sessions are not privileged or protected by professional confidentiality

AI Governance: Managing Data Storage

ROPES & GRAY

- **When managing AI data storage:**
  - Ensure **security and privacy**
    - Establish best practices for network and data security and ensure appropriate levels of security are in place based on the risk/sensitivity of specific data (e.g., protected health information, or "PHI," may require unique considerations)
    - Prepare contingency plans in case of a data breach
    - Implement access controls
    - Use strong authentication
    - Ensure appropriate levels of encryption (both for data "at rest" and data "in transit")
    - Regularly back up data and test backup procedures
    - Take steps to protect personally identifiable information (PII) and comply with privacy regulations
    - Dispose of data securely
    - Document data storage locations
    - Educate and train employees on data security protocols
  - Ensure **quality and integrity**
    - Conduct regular audits to ensure accuracy, completeness, and consistency
    - Implement tools to validate and clean data before it is used for AI model training

AI Governance: Managing Data Storage

ROPES & GRAY

- **When managing data storage generally:**
  - Ensure **compliance with regulations and retention policies**
    - In the context of AI, GenAI tools generate both input and output data ("AI data"), which should be handled with the same care and considerations as other corporate data
    - Ensure familiarity with the physical location of data storage sources as well as what jurisdiction(s) may govern stored data (i.e., GDPR; CCPA; HIPAA, etc.)
    - Questions to consider:
      - What is the purpose of the data storage sites and what kind of data is being stored?
      - Is it a business record? If so, what regulations apply?
      - Where is it stored, and can it be retained?
      - For AI data: Could the AI data fall within a regulated topic or fall under legal preservation holds? If not, what would be the business need for retaining prompts and outputs longer than needed?
  - Ensure appropriate **organization, access, monitoring, and ownership**
    - Categorize data by type, sensitivity, and usage to determine appropriate storage, access controls, and compliance procedures
    - Implement systems to log data access in order to monitor who accesses what data
    - Clearly define who is responsible for data management, security, and compliance

AI Governance: Transcription Considerations

ROPES & GRAY

Given prevalence of enterprise AI tools and ubiquity of video conferencing, employees should assume that all calls and teleconferences are being recorded and/or transcribed

Guidelines for Use of Transcription Tools

- **Consider appropriateness of recording or transcribing a call or meeting**
  - Attorney-Client confidentiality
  - Sensitive information to be discussed, whether trade secrets or legally protected data
  - Will transcription or recording limit participants' comfort to speak freely?
  - DO NOT use for calls on which no employee will participate
  - DO NOT use without the consent of all parties
  - DO confirm whether third party-hosted meetings are being recorded or transcribed
- **Appropriate contractual protections regarding confidentiality**

ROPES & GRAY

Thank you.

BOSTON · CHICAGO · DUBLIN · HONG KONG · LONDON · LOS ANGELES · MILAN · NEW YORK · PARIS

SAN FRANCISCO · SEOUL · SHANGHAI · SILICON VALLEY · SINGAPORE · TOKYO · WASHINGTON, DC