AI Governance for the C-Suite

COV Information Security Conference 2025

Presented by: **Ross M. Broudy, Esq., CIPP/US**
John Pilch, MBA, CIPP/US, CIPP/E, CISSP

August 14, 2025

WoodsRogers

Agenda

I. C-Suite Outlook on AI

II. Introduction to AI Governance

III. Shadow AI, Vendor Management, Security Risks

IV. Implementing AI Governance

V. Legal and Regulatory Update

Ross Broudy
Associate

John Pilch
Senior Cybersecurity / Data Privacy Analyst

Press release

04 Jun 2025 | London, GB

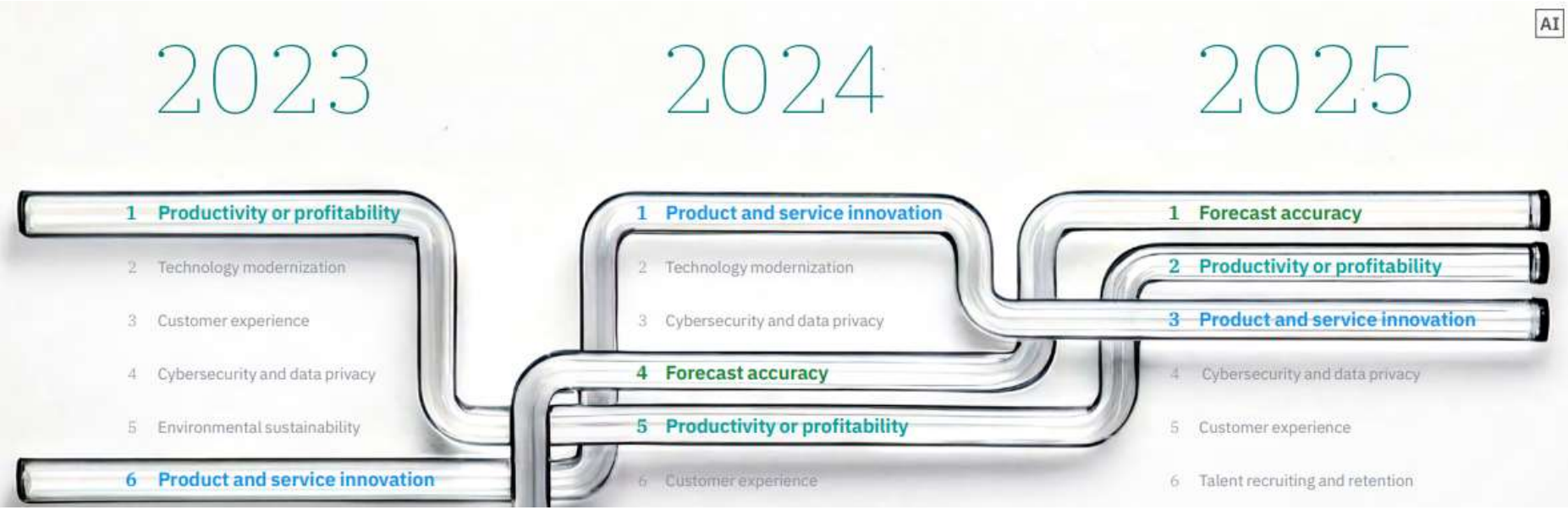
EY survey: AI adoption outpaces governance as risk awareness among the C-suite remains low

- Only a third of companies have responsible controls for current AI models despite nearly three-quarters having AI integrated into initiatives across the organization
- C-suite executives are on average half as worried as consumers about adherence to responsible AI principles
- CEOs show greater concern about AI risks than other C-suite leaders do

Source: EY (June 4, 2025)

Top CEO Priorities in 2025

- AI is rewriting the rules of C-Suite strategy
- #1 high-impact trend for CEOs: the rise of AI and gen AI (Thomas Reuters)
- AI expected to be means of achieving top 3 CEO goals



Source: IBM, 5 mindshifts to supercharge business growth (2025)

The Importance of AI Governance

- Mature AI governance results in better AI outcomes (e.g., productivity, program lifespan)
- Achieve organizational objectives
- Minimize and mitigate legal and regulatory risks
- Minimize and mitigate security risks such as **shadow AI** and increased costs of data breaches

AI Security Risks, By the Numbers

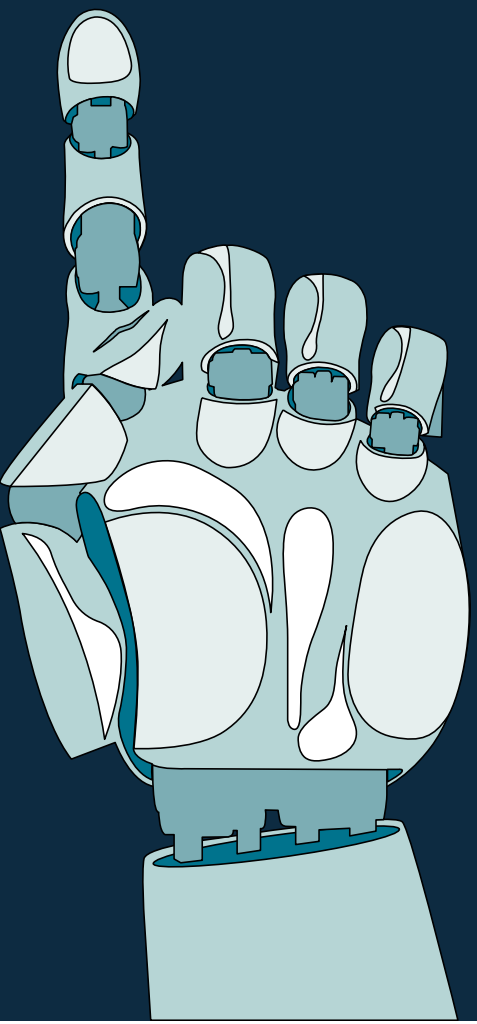
- IBM surveyed 600 organizations affected by data breaches
- 63% lacked AI governance policies
- Only 34% regularly audited for shadow AI (unsanctioned)
- $670K – added breach cost for shadow AI
- 65% more PII and 40% more IP exposed in breaches involving shadow AI
- Takeaway: Ungoverned AI systems are more likely to be breached, are more costly, and may take longer to remediate

Source: IBM – Cost of a Data Breach Report 2025, the AI Oversight Gap (July 2025)

AI Security Risks, By the Numbers

Ungoverned AI systems are more likely to be breached, are more costly, and may take longer to remediate

Source: IBM – Cost of a Data Breach Report 2025, the AI Oversight Gap (July 2025)



Introduction to AI Governance

AI Governance

- A system of frameworks, practices and processes at an organizational level.

- AI governance helps various stakeholders implement, manage and oversee the use of AI technology.

- It also helps
  - manage associated risks to ensure AI aligns with stakeholders' objectives,
  - is developed and used responsibly and ethically,
  - and complies with applicable requirements.

Source: IAPP Key Terms for AI Governance (July 2025)

AI Governance - Evolving Definition

~~June 2023~~July 2025

A system of ~~policies~~frameworks, practices and processes ~~organizations~~at an organizational level. AI governance helps various stakeholders implement ~~to~~, manage and oversee ~~their~~the use of AI technology ~~and~~. It also helps manage associated risks to ensure ~~the~~ AI aligns with ~~an organization's~~stakeholders' objectives, is developed and used responsibly and ethically, and complies with applicable ~~legal~~ requirements.

AI Governance: Example Frameworks

- Frameworks set standards for all phases of AI lifecycle: including development, deployment, monitoring, and decommission

- Some standards recognized by laws such as Colorado AI Act as compliance vehicles

- Examples
  - VITA's Enterprise Architecture Standard 225 (EA-225)
  - NIST: Artificial Intelligence Risk Management Framework (govern, map, measure, manage)
  - ISO/IEC 42:001

AI Governance: MIT AI Risk Mitigation Taxonomy

Figure 1. Draft AI Risk Mitigation Taxonomy

Mitigation Category	Mitigation Subcategory
1. Governance & Oversight Controls *Formal organizational structures and policy frameworks that establish human oversight mechanisms and decision protocols to ensure human accountability, ethical conduct, and risk management throughout AI development and deployment.*	1.1 Board Structure & Oversight
	1.2 Risk Management
	1.3 Conflict of Interest Protections
	1.4 Whistleblower Reporting & Protection
	1.5 Safety Decision Frameworks
	1.6 Environmental Impact Management
	1.7 Societal Impact Assessment
2. Technical & Security Controls *Technical, physical, and engineering safeguards that secure AI systems and constrain model behaviors to ensure security, safety, alignment with human values, and content integrity.*	2.1 Model & Infrastructure Security
	2.2 Model Alignment
	2.3 Model Safety Engineering
	2.4 Content Safety Controls
3. Operational Process Controls *Processes and management frameworks governing AI system deployment, usage, monitoring, incident handling, and validation, which promote safety, security, and accountability throughout the system lifecycle.*	3.1 Testing & Auditing
	3.2 Data Governance
	3.3 Access Management
	3.4 Staged Deployment
	3.5 Post-Deployment Monitoring
	3.6 Incident Response & Recovery
4. Transparency & Accountability Controls *Formal disclosure practices and verification mechanisms that communicate AI system information and enable external scrutiny to build trust, facilitate oversight, and ensure accountability to users, regulators, and the public.*	4.1 System Documentation
	4.2 Risk Disclosure
	4.3 Incident Reporting
	4.4 Governance Disclosure
	4.5 Third-Party System Access
	4.6 User Rights & Recourse

Source: MIT (July 2025)

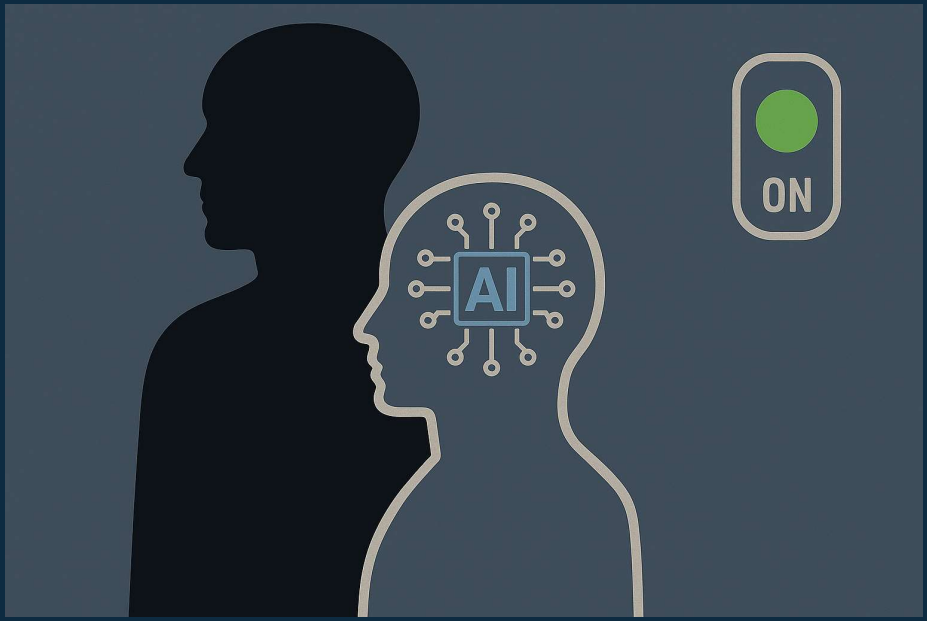
AI Governance: MIT AI Risk Mitigation Taxonomy

Appendix A: Draft AI Risk Mitigation Taxonomy

Mitigation Category	Mitigation Subcategory	Subcategory description	Examples
1. Governance & Oversight Controls *Formal organizational structures and policy frameworks that establish human oversight mechanisms and decision protocols to ensure human accountability, ethical conduct, and risk management throughout AI development and deployment.*	1.1 Board Structure & Oversight	Governance structures and leadership roles that establish executive accountability for AI safety and risk management.	*Dedicated risk committees, safety teams, ethics boards, crisis simulation training, multi-party authorization protocols, deployment veto powers*
	1.2 Risk Management	Systematic methods that identify, evaluate, and manage AI risks for comprehensive risk governance across organizations.	*Enterprise risk management frameworks, risk registers with capability thresholds, compliance programs, pre-deployment risk assessments, independent risk assessments*
	1.3 Conflict of Interest Protections	Governance mechanisms that manage financial interests and organizational structures to ensure leadership can prioritize safety over profit motives in critical situations.	*Background checks for key personnel, windfall profit redistribution plans, stake limitation policies, protections against shareholder pressure*
	1.4 Whistleblower Reporting & Protection	Policies and systems that enable confidential reporting of safety concerns or ethical violations to prevent retaliation and encourage disclosure of risks.	*Anonymous reporting channels, non-retaliation guarantees, limitations on non-disparagement agreements, external whistleblower handling services*
	1.5 Safety Decision Frameworks	Protocols and commitments that constrain decision-making about model development, deployment, and capability scaling, and govern safety-capability resource allocation to prevent unsafe AI advancement.	*If-then safety protocols, capability ceilings, deployment pause triggers, safety-capability resource ratios*
	1.6 Environmental Impact Management	Processes for measuring, reporting, and reducing the environmental footprint of AI systems to ensure sustainability and responsible resource use.	*Carbon footprint assessment, emission offset programs, energy efficiency optimization, resource consumption tracking*
	1.7 Societal Impact Assessment	Processes that assess AI systems' effects on society, including impacts on employment, power dynamics, political processes, and cultural values.	*Fundamental rights impact assessments, expert consultations on risk domains, stakeholder engagement processes, governance gap analyses*

Source: MIT (July 2025)

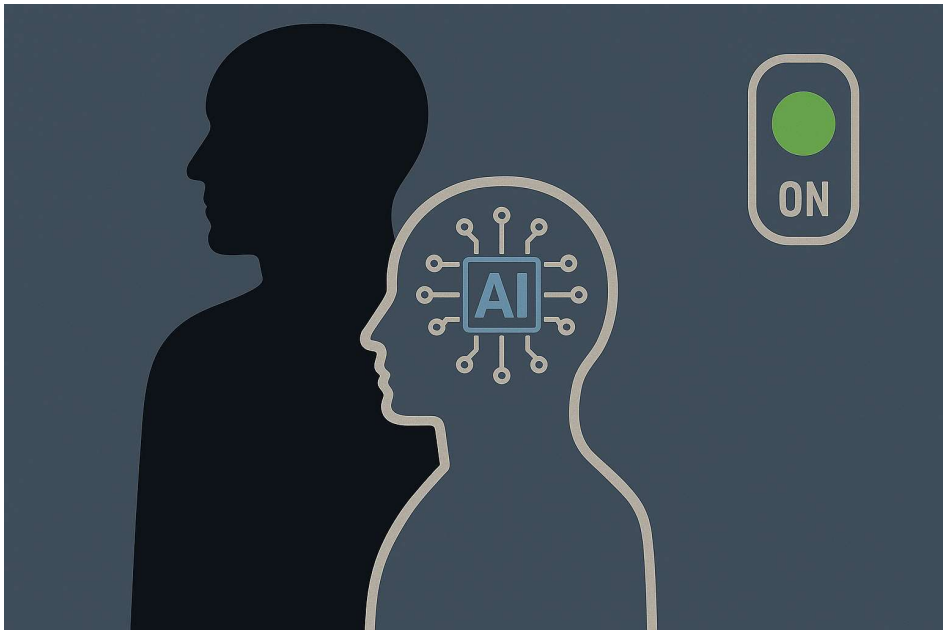
Shadow AI, Vendor Management, Security Risks



What is Shadow AI?

- “Unauthorized use of AI systems in an organization, often against organizational policies for data governance, privacy, and AI use”
- Can be internal (employees) or external (vendors)
- Examples
  - Internal – employee using ChatGPT to analyze proprietary data
  - External – SaaS vendor ingesting company data into their GenAI

Sources: IBM (Oct. 25, 2024); IAPP Key Terms



Copilot Prompt:
Generate a picture of "shadow artificial intelligence turned on secretly by SaaS vendor" to be included in a presentation on AI governance for the C-Suite. The graphic should not have any words.

Accuracy and Hallucinations: OpenAI's Terms of Use and Services Agreement (fka Business Terms)

Updated: December 11, 2024

Terms of Use

Accuracy. Artificial intelligence and machine learning are rapidly evolving fields of study. We are constantly working to improve our Services to make them more accurate, reliable, safe, and beneficial. Given the probabilistic nature of machine learning, use of our Services may, in some situations, result in Output that does not accurately reflect real people, places, or facts.

When you use our Services you understand and agree:

- Output may not always be accurate. You should not rely on Output from our Services as a sole source of truth or factual information, or as a substitute for professional advice.
- You must evaluate Output for accuracy and appropriateness for your use case, including using human review as appropriate, before using or sharing Output from the Services.
- You must not use any Output relating to a person for any purpose that could have a legal or material impact on that person, such as making credit, educational, employment, housing, insurance, legal, medical, or other important decisions about them.

OpenAI

Effective: May 31, 2025

OpenAI Services Agreement

Download PDF ↗ View previous business terms >

- 4.3. Customer Obligations. Customer is responsible for all Input and represents and warrants that it has all rights, licenses, and permissions required to provide Input to the Services. Customer is solely responsible for all use of the Outputs and for evaluating the accuracy and appropriateness of Output for Customer's use case.

Content and Model Training: OpenAI's Terms of Use and Services Agreement (fka Business Terms)

Updated: December 11, 2024

Terms of Use

Content

Your content. You may provide input to the Services ("Input"), and receive output from the Services based on the Input ("Output"). Input and Output are collectively "Content." You are responsible for Content, including ensuring that it does not violate any applicable law or these Terms. You represent and warrant that you have all rights, licenses, and permissions needed to provide Input to our Services.

Our use of content. We may use Content to provide, maintain, develop, and improve our Services, comply with applicable law, enforce our terms and policies, and keep our Services safe. If you're using ChatGPT through Apple's integrations, see this Help Center article for how we handle your Content.

Opt out. If you do not want us to use your Content to train our models, you can opt out by following the instructions in this Help Center article. Please note that in some cases this may limit the ability of our Services to better address your specific use case.

OpenAI

Effective: May 31, 2025

OpenAI Services Agreement

Download PDF ↗ View previous business terms >

4. Customer Content.

- 4.1. Generally. Customer and Customer's End Users may provide Input and receive Output. As between Customer and OpenAI, to the extent permitted by applicable law, Customer: (a) retains all ownership rights in Input; and (b) owns all Output. OpenAI hereby assigns to Customer all OpenAI's right, title, and interest, if any, in and to Output.
- 4.2. OpenAI Obligations. OpenAI will only use Customer Content as necessary to provide Customer with the Services, comply with applicable law, enforce the OpenAI Policies, and prevent abuse. OpenAI will not use Customer Content to develop or improve the Services, unless Customer explicitly agrees to such use.

Ownership

You own and control your data

- ✓ We do not train our models on your business data by default
- ✓ You own your inputs and outputs (where allowed by law)
- ✓ You control how long your data is

Vendor Management

- Required contract terms (e.g., Virginia Consumer Data Protection Act)
- Focus on key liability provisions (limitation of liability, indemnification, damages waivers)
- “Sales materials” versus representations/warranties
- AI Appendix or Supplement

Required Contract Terms (Va. Code § 59.1-579)

Contract between controller processor governs the processor's data processing procedures regarding processing performed on behalf of controller.

Binding contract that shall clearly set forth

- Instructions for processing data
- Nature and purpose of processing
- Type of data subject to processing
- Duration of processing
- All rights and obligations of both parties

Minimum contractual requirements that processor shall:

1. Ensure each person processing personal data is subject to a **duty of confidentiality**
2. At controller's direction, delete or return all personal data to controller as requested at the end of the provision of services, unless retention is required by law
3. Upon reasonable request of controller, make available all information in its possession necessary to demonstrate processor's compliance with state CDPA
4. Allow and cooperate with reasonable assessments by the controller or designee; alternatively, processor may arrange for a qualified independent assessor to assess processor's policies and technical/organizational measures using an appropriate control standard. The processor shall provide a report to controller at their request.
5. Engage any subcontractor pursuant to written contract that requires subcontractor to meet processor's personal data obligations.

NVIDIA Software License Agreement

Last Modified: May 5, 2025

17.27 "Model" means any Software that is a machine-learning based assembly (including checkpoints), consisting of learnt weights, parameters (including optimizer states) and configuration files that may be trained or tuned, in whole or in part, on data.

11. **DATA COLLECTION.**

11.1 Collection Purposes. Customer acknowledges that Software may collect data for the following purposes: (a) properly configure and optimize products for use with Software; (b) deliver content or service through the Software; (c) check for compliance with the license or detect fraud or other malicious activity; and (d) improve NVIDIA products and services. Information collected may include: (i) configuration data; (ii) operating system; (iii) installed applications and drivers used with Software; and (iv) application settings, performance and usage data. With Customer's consent, diagnostic data, including crash reports, may be collected. Further, NVIDIA may require certain personal information such as name, email address and entitlement information to deliver Software or provide Services to Customer. Please review documentation accompanying the relevant Software for data collection specific to the Software.

14. **LIMITATION OF LIABILITY.**

14.1 Disclaimers. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY (I) INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR (II) DAMAGES FOR THE (A) COST OF PROCURING SUBSTITUTE GOODS, OR (B) LOST PROFITS, REVENUE, USE, DATA OR GOODWILL ARISING OUT OF OR IN CONNECTION WITH THE AGREEMENT OR THE USE OR THE PERFORMANCE OF SOFTWARE OFFERINGS WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, AND EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A PARTY'S REMEDIES FAIL THEIR ESSENTIAL PURPOSE.

14.2 Damages Capped. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NVIDIA'S TOTAL CUMULATIVE AGGREGATE LIABILITY FOR ANY AND ALL LIABILITIES, OBLIGATIONS OR CLAIMS ARISING OUT OF OR RELATED TO THE AGREEMENT WILL NOT EXCEED THE NET AMOUNT NVIDIA WAS PAID FOR THE SOFTWARE GIVING RISE TO THE CLAIM DURING THE TWELVE (12) MONTHS PERIOD BEFORE THE EVENT GIVING RISE TO THE LIABILITY (OR UP TO US$100.00 IF CUSTOMER OBTAINED SUCH SOFTWARE AT NO CHARGE).

Security: MIT AI Risk Mitigation Taxonomy

Mitigation Category	Mitigation Subcategory	Subcategory description	Examples
2. Technical & Security Controls *Technical, physical, and engineering safeguards that secure AI systems and constrain model behaviors to ensure security, safety, alignment with human values, and content integrity.*	2.1 Model & Infrastructure Security	Technical and physical safeguards that secure AI models, weights, and infrastructure to prevent unauthorized access, theft, tampering, and espionage.	*Model weight tracking systems, multifactor authentication protocols, physical access controls, background security checks, compliance with information security standards*
	2.2 Model Alignment	Technical methods to ensure AI systems understand and adhere to human values and intentions.	*Reinforcement learning from human feedback (RLHF), direct preference optimization (DPO), constitutional AI training, value alignment verification systems*
	2.3 Model Safety Engineering	Technical methods and safeguards that constrain model behaviors and protect against exploitation and vulnerabilities.	*Safety analysis protocols, capability restriction mechanisms, hazardous knowledge unlearning techniques, input/output filtering systems, defense-in-depth implementations, adversarial robustness training, hierarchical auditing, action replacement*
	2.4 Content Safety Controls	Technical systems and processes that detect, filter, and label AI-generated content to identify misuse and enable content provenance tracking.	*Synthetic media watermarking, content filtering mechanisms, prohibited content detection, metadata tagging protocols, deepfake creation restrictions*

Source: MIT (July 2025)

Deepfakes

TECHNOLOGY

Creating realistic deepfakes is getting easier than ever. Fighting back may take even more AI

AP

BY DAVID KLEPPER
Updated 7:17 AM EDT, July 28, 2025

Share

WASHINGTON (AP) — The phone rings. It's the secretary of state calling. Or is it?

For Washington insiders, seeing and hearing is no longer believing, thanks to a spate of recent incidents involving deepfakes impersonating top officials in President Donald Trump's administration.

Digital fakes are coming for corporate America, too, as criminal gangs and hackers associated with adversaries including North Korea use synthetic video and audio to impersonate CEOs and low-level job candidates to gain access to critical systems or business secrets.

Thanks to advances in artificial intelligence, creating realistic deepfakes is easier than ever, causing security problems for governments, businesses and private individuals and making trust the most valuable currency of the digital age.

Responding to the challenge will require laws, better digital literacy and technical solutions that fight AI with more AI.

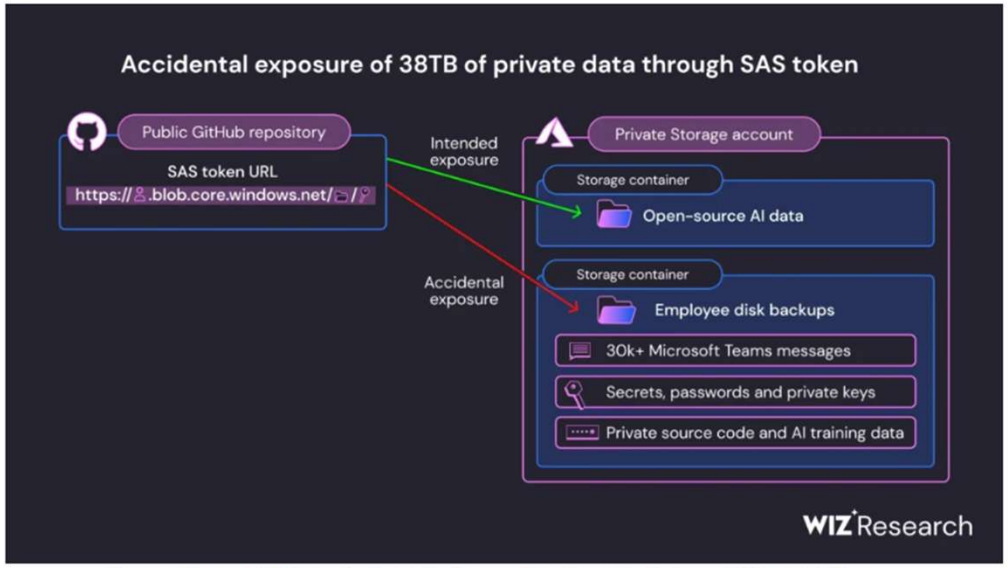
Data Privacy AI Risks

ARTIFICIAL INTELLIGENCE

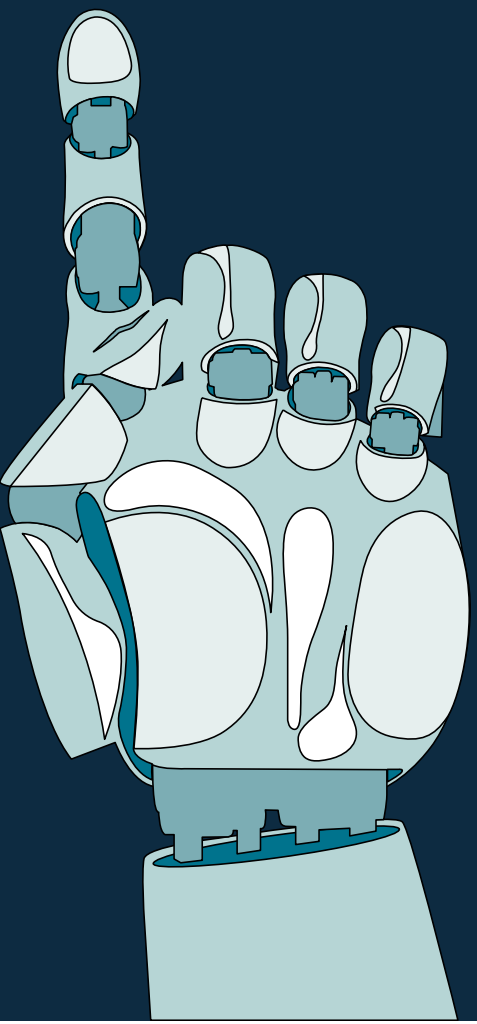
Microsoft AI Researchers Expose 38TB of Data, Including Keys, Passwords and Internal Messages

Exposed data includes backup of employees workstations, secrets, private keys, passwords, and over 30,000 internal Microsoft Teams messages.

By Ryan Naraine
September 18, 2023



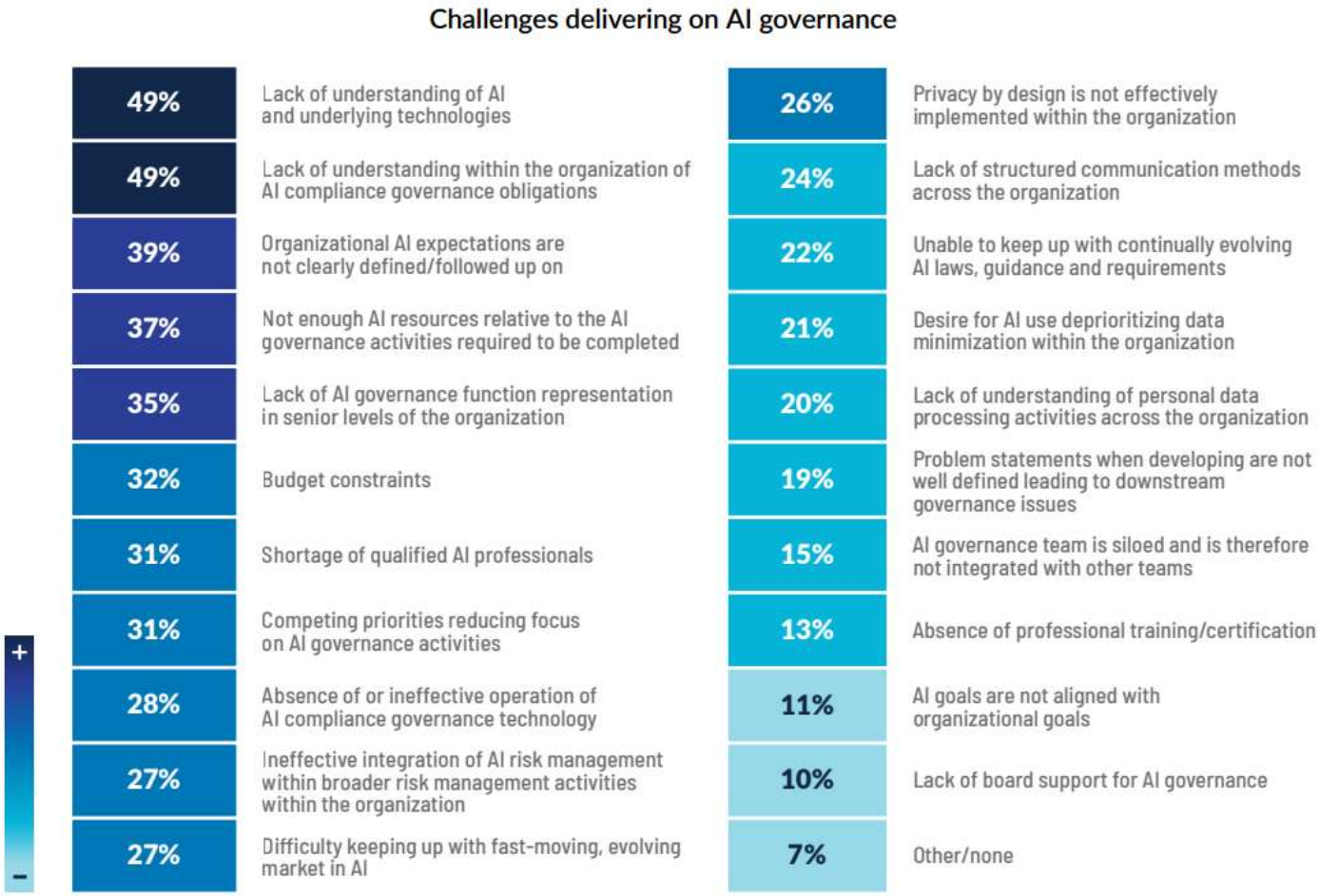
Researchers at Wiz have flagged another major security misstep at Microsoft that caused the exposure of 38 terabytes of private data during a routine open source AI training material update on GitHub.



Implementing AI Governance

What is your organization's top challenge in delivering on AI governance?

Challenges in Implementing AI Governance (2025)



Source: IAPP/Credo AI (April 2025)

Board Structure & Oversight

Appendix A: Draft AI Risk Mitigation Taxonomy

Mitigation Category	Mitigation Subcategory	Subcategory description	Examples
1. Governance & Oversight Controls *Formal organizational structures and policy frameworks that establish human oversight mechanisms and decision protocols to ensure human accountability, ethical conduct, and risk management throughout AI development and deployment.*	1.1 Board Structure & Oversight	Governance structures and leadership roles that establish executive accountability for AI safety and risk management.	*Dedicated risk committees, safety teams, ethics boards, crisis simulation training, multi-party authorization protocols, deployment veto powers*
	1.2 Risk Management	Systematic methods that identify, evaluate, and manage AI risks for comprehensive risk governance across organizations.	*Enterprise risk management frameworks, risk registers with capability thresholds, compliance programs, pre-deployment risk assessments, independent risk assessments*
	1.3 Conflict of Interest Protections	Governance mechanisms that manage financial interests and organizational structures to ensure leadership can prioritize safety over profit motives in critical situations.	*Background checks for key personnel, windfall profit redistribution plans, stake limitation policies, protections against shareholder pressure*
	1.4 Whistleblower Reporting & Protection	Policies and systems that enable confidential reporting of safety concerns or ethical violations to prevent retaliation and encourage disclosure of risks.	*Anonymous reporting channels, non-retaliation guarantees, limitations on non-disparagement agreements, external whistleblower handling services*
	1.5 Safety Decision Frameworks	Protocols and commitments that constrain decision-making about model development, deployment, and capability scaling, and govern safety-capability resource allocation to prevent unsafe AI advancement.	*If-then safety protocols, capability ceilings, deployment pause triggers, safety-capability resource ratios*
	1.6 Environmental Impact Management	Processes for measuring, reporting, and reducing the environmental footprint of AI systems to ensure sustainability and responsible resource use.	*Carbon footprint assessment, emission offset programs, energy efficiency optimization, resource consumption tracking*
	1.7 Societal Impact Assessment	Processes that assess AI systems' effects on society, including impacts on employment, power dynamics, political processes, and cultural values.	*Fundamental rights impact assessments, expert consultations on risk domains, stakeholder engagement processes, governance gap analyses*

Source: MIT (July 2025)

AI Governance Committee

- Cross functional team, comprised of key players (e.g., CISO, chief privacy officer, HR director)
- May report directly to the CEO or full C-Suite
- Top uses of AI governance committees:
  - PR/Communications
  - Vendor Management
  - Product Development
  - HR
  - Audit/Internal Control

Source: IAPP/Credo AI (April 2025)

AI Risk Mitigation Officer

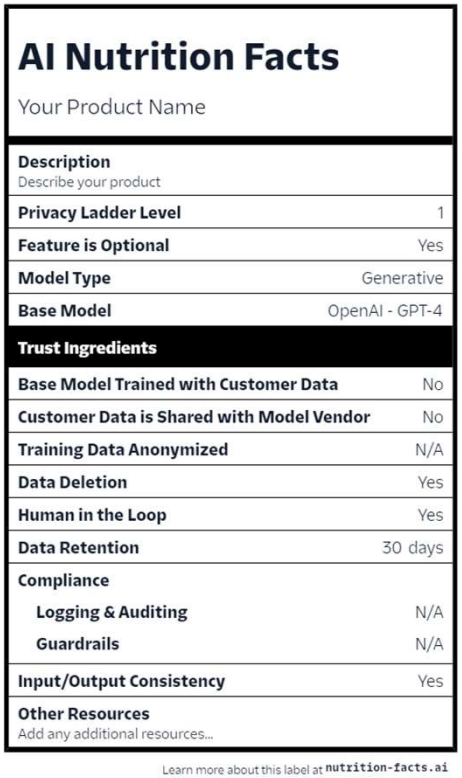
Navigating AI's Twin Perils: The Rise of the Risk-Mitigation Officer

RALPH LOSEY / JULY 23, 2025 / AI ETHICS, AI INSTRUCTION, BLOG ARTICLES, CHATGPT, IN THE NEWS, INTERNET REGULATION, KNOWLEDGE, LAWYERS DUTIES, RECENT NEWS, TECHNOLOGY, WISDOM

Source: EDRM, Ralph Losey (July 23, 2025)

AI Governance: Accountability

- Start with framework
- Consult laws on the books (even if not applicable)
- Develop effective AI “Playbooks”
- Constant monitoring, continuous assessment
- Policies and standards
  - Inventories
  - Design documentation
  - Risk assessments
  - Developer guidelines (vendors and internal)



AI Nutrition Facts

Your Product Name

Description Describe your product	
Privacy Ladder Level	1
Feature is Optional	Yes
Model Type	Generative
Base Model	OpenAI - GPT-4
Trust Ingredients	
Base Model Trained with Customer Data	No
Customer Data is Shared with Model Vendor	No
Training Data Anonymized	N/A
Data Deletion	Yes
Human in the Loop	Yes
Data Retention	30 days
Compliance	
Logging & Auditing	N/A
Guardrails	N/A
Input/Output Consistency	Yes
Other Resources Add any additional resources...	

Learn more about this label at nutrition-facts.ai

Source: https://nutrition-facts.ai/

AI Service Card Example

- How it Works
- Architecture
- Model Details
- No Training on Customer Data
- Known Limitations
- Guardrails
  - Monitoring
  - Fairness and Bias
  - Explainability and Transparency
  - Accountability

Hyland IDP

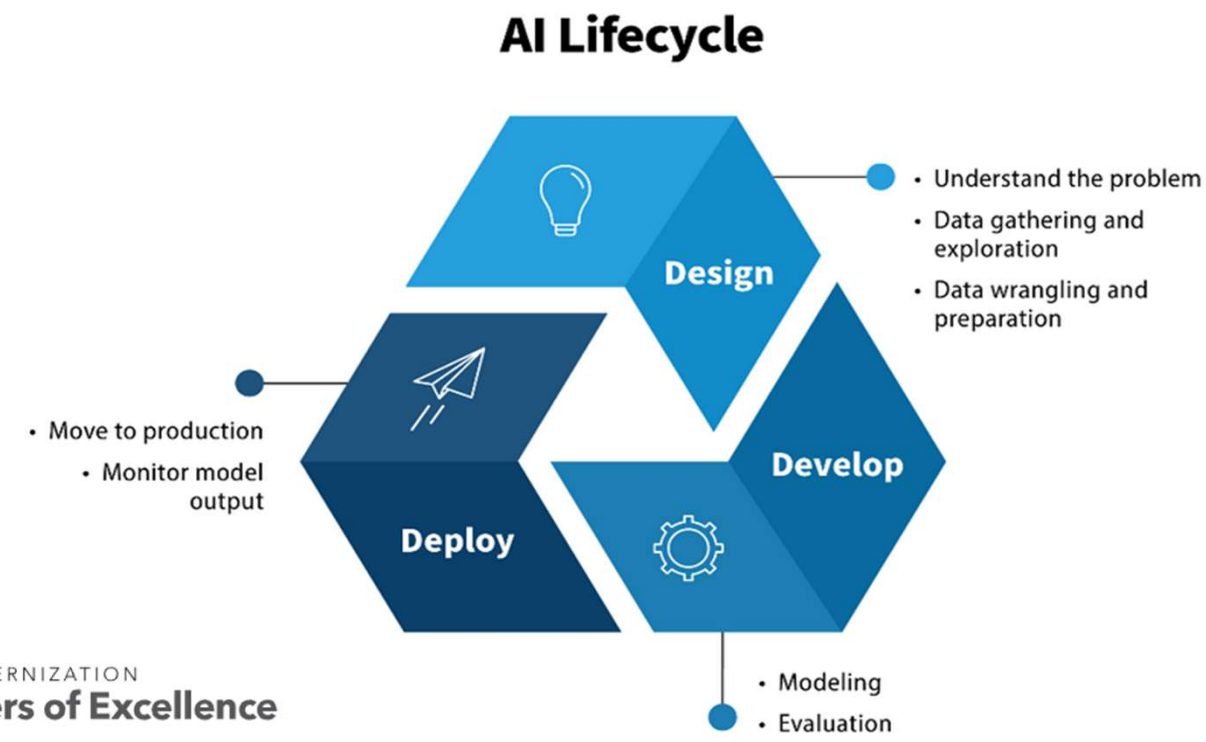
AI Service Card

v.2

Intended Use

Hyland IDP is an intelligent document processing software that delivers AI-powered agentic document processing including AI-powered document capture, separation, classification and intelligent data extraction and enrichment. Hyland IDP leverages large language models (LLMs) with generative AI (gen AI) to power document processing and simplify automation design and configuration with dynamic suggestions, prebuilt templates, low-code configuration and automatic business process model and notation (BPMN)-compliant process generation.

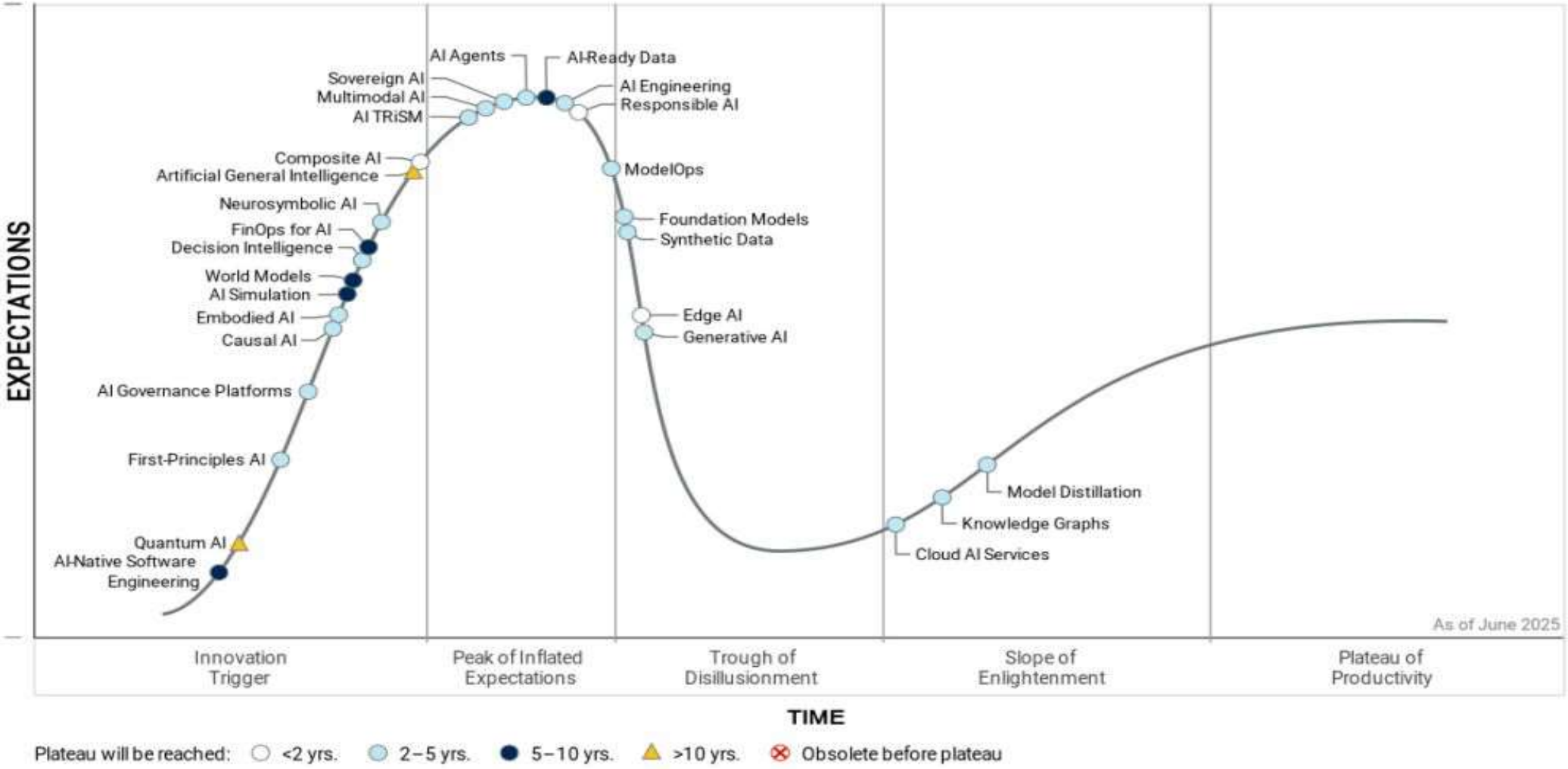
Operationalizing AI



IT MODERNIZATION
Centers of Excellence

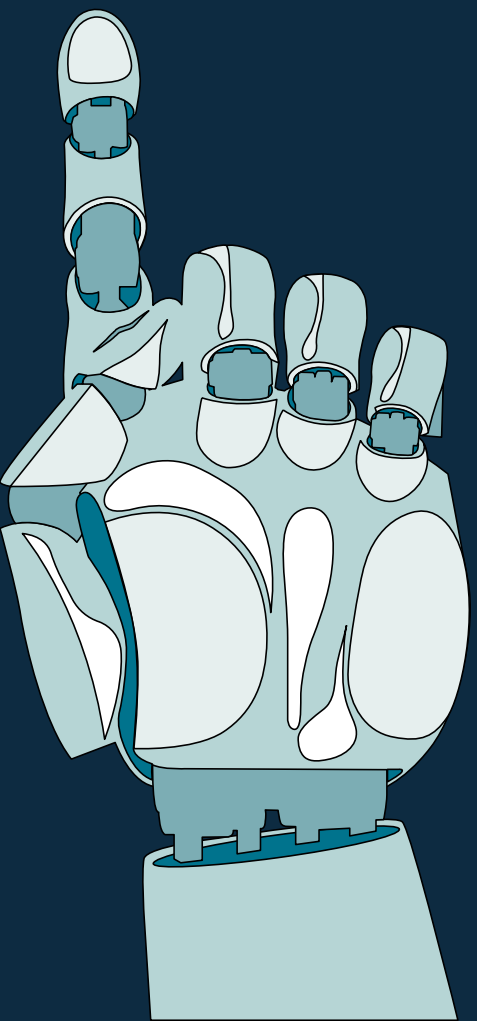
Source: U.S. General Services Administration, Centers of Excellence

Hype Cycle for Artificial Intelligence, 2025



Plateau will be reached: ○ <2 yrs. ● 2–5 yrs. ● 5–10 yrs. ▲ >10 yrs. ⊗ Obsolete before plateau

Gartner



Legal and Regulatory Update

The Race to Regulate AI

- Executive Orders (State and Federal)
- Federal Regulatory Enforcement
- Ongoing Rulemaking
- Federal Legislative Activity
- State Regulatory Frameworks
- State Legislative Activity
- International Law
- Self-Regulatory Commitments, Attestations to Frameworks
- Non-Binding Policy Directives or Initiatives

Source: *AI Check-Up: Regulatory Prognosis for AI/ML in Healthcare*, Maggie Hanjani, Anushree Nakkana, Gregory Stein, & Alya Sulaiman, IAPP AIGG23 (November 2023)

State AI Developments:

Regulations, Legislation, Executive Orders

California

Pending Regulations

CPPA

MODIFIED TEXT OF PROPOSED REGULATIONS

TITLE 11. LAW
DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY
CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

Colorado

Colorado AI Act

Effective: May 17, 2024

C.R.S.A. § 6-1-1701

§ 6-1-1701. Definitions

(3) "CONSEQUENTIAL DECISION" MEANS A DECISION THAT HAS A MATERIAL LEGAL OR SIMILARLY SIGNIFICANT EFFECT ON THE PROVISION OR DENIAL TO ANY CONSUMER OF, OR THE COST OR TERMS OF:

(a) EDUCATION ENROLLMENT OR AN EDUCATION OPPORTUNITY;

(b) EMPLOYMENT OR AN EMPLOYMENT OPPORTUNITY;

(c) A FINANCIAL OR LENDING SERVICE;

Virginia

Executive Orders

Executive Order
NUMBER THIRTY (2024)

IMPLEMENTATION OF STANDARDS FOR THE SAFE USE OF ARTIFICIAL INTELLIGENCE ACROSS THE COMMONWEALTH

By virtue of the authority vested in me as Governor, I hereby issue this Executive Order to promulgate important safety standards to ensure the responsible, ethical, and transparent use of artificial intelligence technology by state government in order to protect the rights of Virginians, to provide best-in-class state government services, and to ensure that our students are well prepared for this technology.

Executive Order
NUMBER FIFTY-ONE (2025)

FIRST-IN-THE-NATION AGENTIC ARTIFICIAL INTELLIGENCE (AI) EMPOWERED STATEWIDE REGULATORY REVIEW

By virtue of the authority vested in me as Governor under Article V of the Constitution of the Commonwealth of Virginia and under the laws of the Commonwealth, I hereby establish in this Executive Order the nation's first statewide agentic AI-powered regulatory review to ensure the Commonwealth captures the benefits of AI in reducing regulatory burdens and keeping regulations and guidance documents streamlined and up-to-date.

State Level: Colorado AI Act

- Colorado's "Consumer Protections for Interactions with Artificial Intelligence" law was enacted on May 17, 2024. Expected to go into effect February 1, 2026.

- Requires "**developers and entities**" that deploy "**high-risk AI systems**" to use **reasonable care** to prevent algorithmic discrimination.
  - High-risk AI system defined as **those that make or are a substantial factor in making "consequential" decisions.** Defines a "substantial factor" as a factor that (i) assists in making a consequential decision, (ii) is capable of altering the outcome of a substantial decision, or (iii) is generated by an AI system.
  - **Consequential decision** defined as a decision that has a "**material legal or similarly significant effect"** on the provision or denial to any consumer of, or the cost or terms of, education
    - Education enrollment or opportunity, Employment or employment opportunity, Financial or lending services, Essential government service, Health care services, Housing, Insurance, Legal services

- Proposed Virginia law HB2094 similar to Colorado AI Act was vetoed

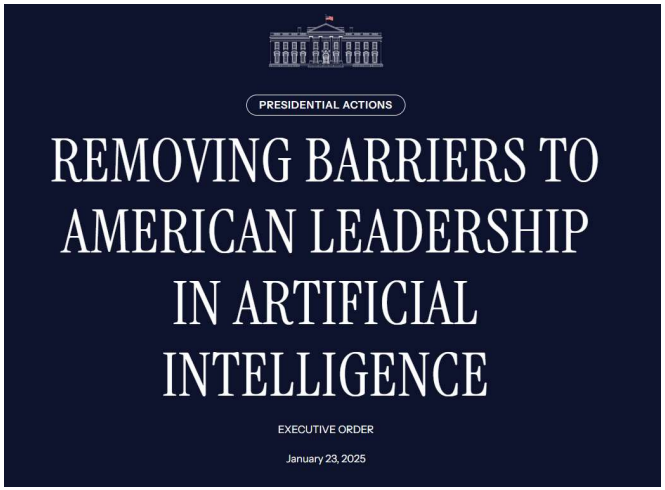
Source: SB205

Slide 37

EP0 Removed colon after “or the cost and terms of: education” and instead inserted a comma
Erin Pope, 2025-08-06T13:30:09.254

The Race to Regulate AI: Federal Level

- **Executive Order (Jan. 23, 2025)**
  - Titled: Removing Barriers to American Leadership in AI
  - EO 14110 rescinded on Jan. 20, 2025
  - Policy objective: "to sustain and enhance **America's global AI dominance** in order to promote **human flourishing**, **economic competitiveness**, and **national security**."
- **White House AI Action Plan (July 2025)**
  - Pillar I: Accelerate AI Innovation
  - Pillar II: Build American AI Infrastructure
  - Pillar III: Lead in International AI Diplomacy and Security



Existing Law Applies to AI

“There is no AI exemption from the laws on the books…”

-Lina M. Khan, FTC Chair

Source: Remarks of Chair Lina M. Khan, FTC Tech Summit (Jan. 25, 2024)

AI Core Substantive Legal Risks

Data Privacy and Security

Tort Liability

IP

Consumer Protection

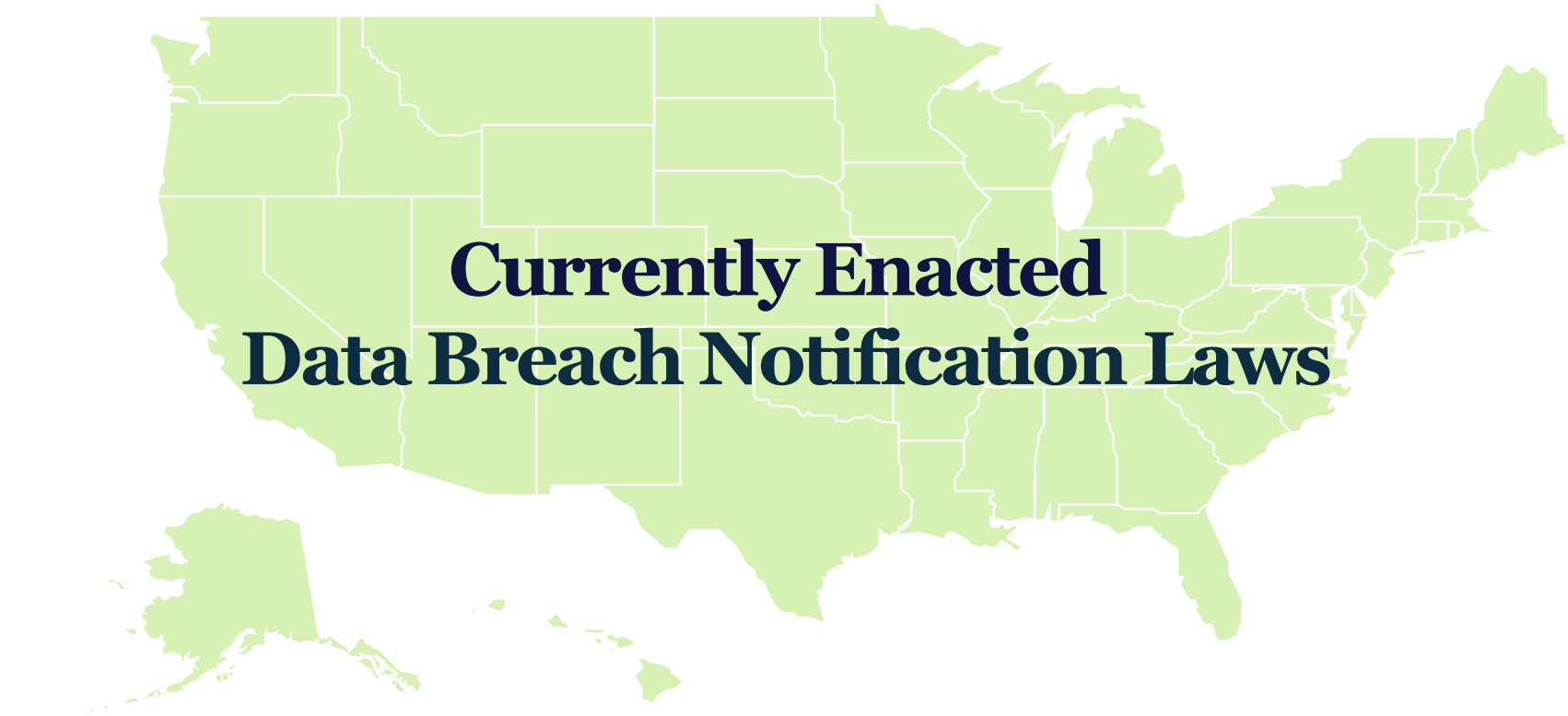
Discrimination and Bias

Contract Liability

Data Privacy AI Risks: Personally Identifiable Information ("PII")

Name plus… SSN, driver's license ID, financial account with pin, or passport number

See e.g. Va. Code § 18.2-186.6



AI Discrimination and Bias

EEOC v. iTutorGroup Inc.

U.S. Equal Employment Opportunity Commission

Press Release
09-11-2023

iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit

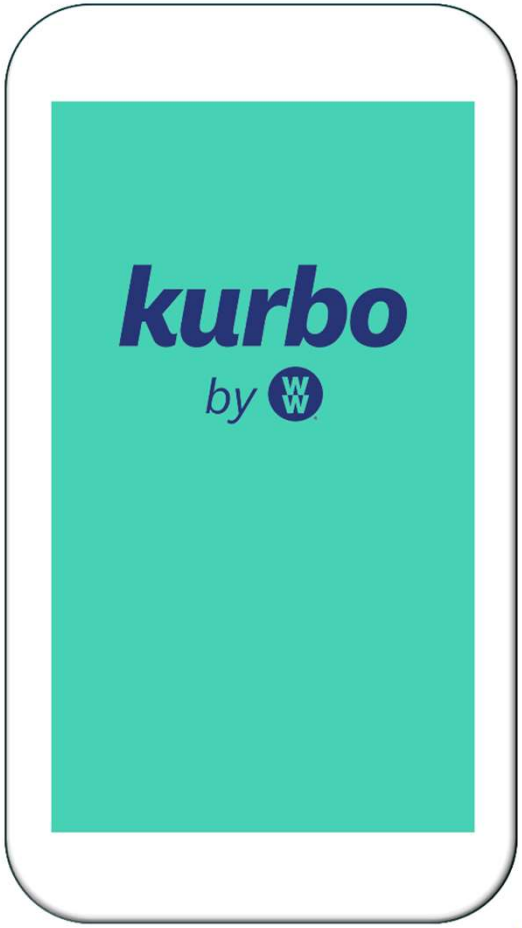
Settles Federal Charges Tutoring Provider Programmed its Online Software to Automatically Reject More Than 200 Older Applicants

NEW YORK – iTutorGroup, three integrated companies providing English-language tutoring services to students in China, will pay $365,000 and furnish other relief to settle an employment discrimination lawsuit filed by the U.S. Equal Employment Opportunity Commission (EEOC), the federal agency announced today.

Sources: EEOC (Sept. 11, 2023); Equal Employment Opportunity Commission v. iTutorGroup, Inc. et al, Docket No. 1:22-cv-02565 (E.D.N.Y. May 05, 2022), Court Docket

Consumer Protection: FTC v. Kurbo (Weight Watchers)

- WW marketed a weight loss app for children
- FTC alleged WW collected and stored children's PII w/o notice or parent consent
  - Violation of Children's Online Privacy Protection Act Rule (COPPA)
- In settlement, WW ordered to pay $1.5M, delete data, destroy algorithms that used data



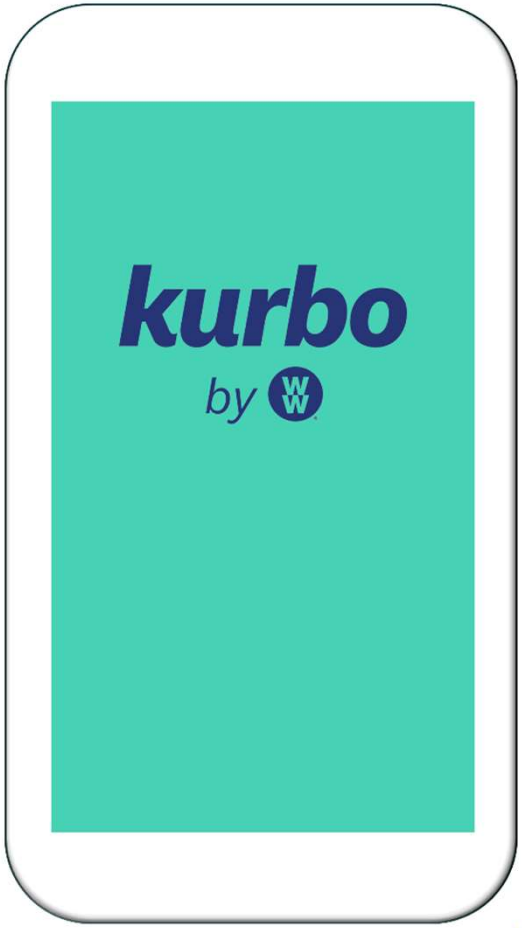
Sources:

- *United States v. Kurbo*, 3:22-cv-00946 (N.D. Cal. 2022), complaint, Complaint (ftc.gov), Stipulated Order, Weight Watchers/Kurbo: Stipulated Order (ftc.gov)
- *FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids Sensitive Health Data*, FTC (March 4, 2022), FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data | Federal Trade Commission

Consumer Protection: FTC v. Kurbo (Weight Watchers)

"'Model deletion' also referred to interchangeably as model or algorithmic disgorgement, algorithmic destruction, and model deletion, is the ***compelled destruction or dispossession*** of data, algorithms, models, and associated work products that are created or shaped by illegal means."

Source: Jevan Hutson & Ben Winters, *America's Next "Stop Model!": Model Deletion,* 1 GEORGETOWN LAW TECH. REV. 124, 128-29 (Jan. 2024).



Consumer Protection: Model Deletion

In re X-Mode Social (Jan. 9, 2024)

D. "**Data Product**" means any model, algorithm or derived data, in Respondents' custody or control developed, in whole or part, using Historic Location Data. Data Product includes but is not limited to any derived data produced via inference (manual or automated) or predictions such as audience segments.

F. "**Historic Location Data**" means any Location Data that Respondents collected from consumers without consumers' Affirmative Express Consent.

XIII. Deletion

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must, unless prohibited by law:

C. Within 90 days after the effective date of this Order, delete or destroy all Data Products, and provide a written statement to the Commission, pursuant to Provision XVII, confirming such deletion or destruction.

Source: *In re X-Mode Social, Inc.* (Jan. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-Mode-D%26O.pdf

The Race to Regulate AI

- Executive Orders (State and Federal)
- Federal Regulatory Enforcement
- Ongoing Rulemaking
- Federal Legislative Activity
- State Regulatory Frameworks
- State Legislative Activity
- International Law
- Self-Regulatory Commitments, Attestations to Frameworks
- Non-Binding Policy Directives or Initiatives

Source: *AI Check-Up: Regulatory Prognosis for AI/ML in Healthcare*, Maggie Hanjani, Anushree Nakkana, Gregory Stein, & Alya Sulaiman, IAPP AIGG23 (November 2023)

Ross Broudy
Associate

John Pilch
Senior Cybersecurity / Data Privacy Analyst

Ross M. Broudy

Associate, Cybersecurity & Data Privacy

ross.broudy@woodsrogers.com

757.446.8659

John Pilch

Senior Cybersecurity / Data Privacy Analyst

john.pilch@woodsrogers.com

WoodsRogers