



Staying Ahead of AI Legislation: Key Steps to Prepare for Future Privacy Risks



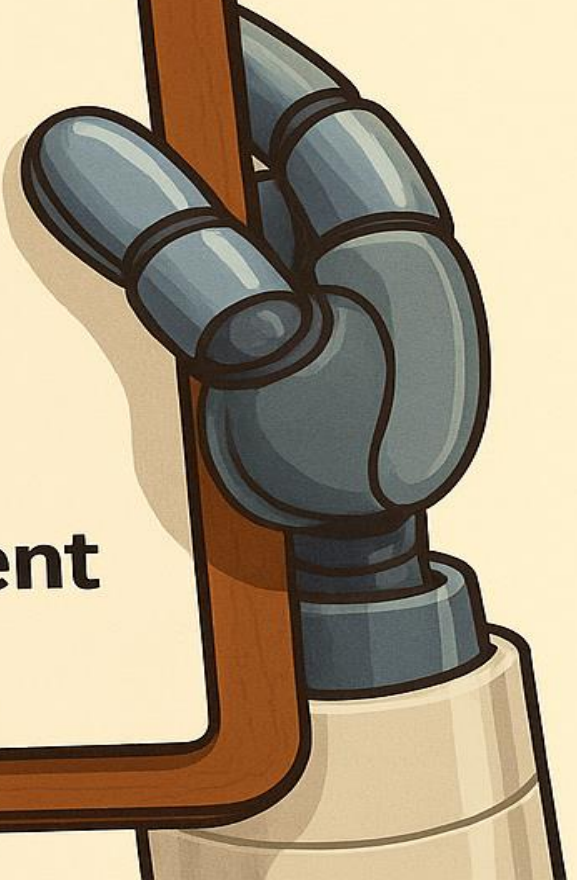
**David J. Walton, AIGP,
CIPP/US**
Partner | Philadelphia
dwalton@fisherphillips.com
610.230.6105



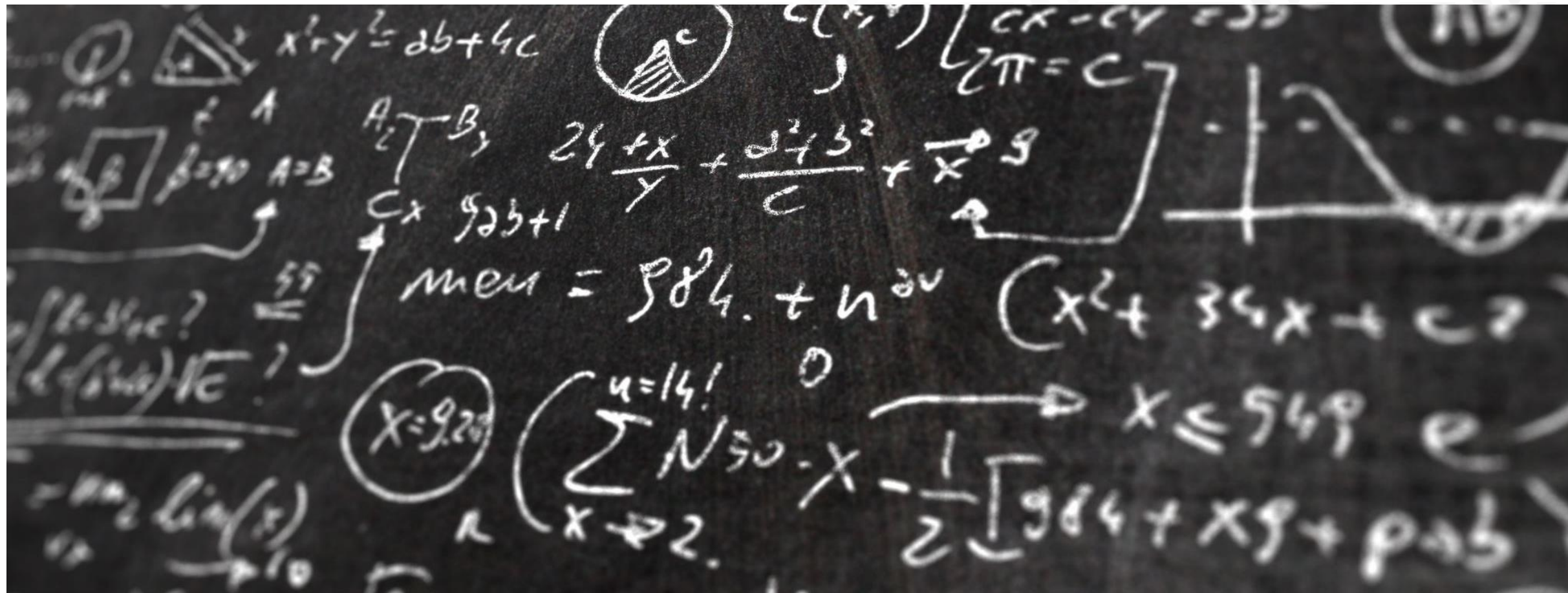
Risa B. Boerner, CIPP/US, CIPM
Partner | Philadelphia
rboerner@fisherphillips.com
610.230.2132

Agenda

- ☐ Intro + Big Picture
- ☐ Legal Landscape: Privacy + AI Employment Laws
- ☐ Privacy Risks & Rights
- ☐ AI Discrimination & Bias
- ☐ Security Risks
- ☐ Governance + Vendor Management
- ☐ Practical Tips & Checklists



Introduction and Big Picture



AI is Transformational

- AI is like electricity and the Internet.
- AI is a general-purpose technology.
- Many innovations are fit for one purpose (e.g., rockets; medical advancements).
- AI's impact is broader; it affects everything from generating art to autonomous vehicles to developing the most efficient delivery routes.



Understanding the Overlap: AI & Privacy



- **How AI Implicates Privacy**
 - AI models depend on large datasets (often personal or sensitive data)
 - Privacy risks arise in training, deployment, and output
- **Types of AI That Trigger Privacy Concerns**
 - Generative AI (e.g., ChatGPT, image/video generators)
 - Automated decision-making tools (e.g., resume screeners)
 - Predictive analytics and surveillance tools

LEGAL LANDSCAPE



State Consumer Privacy Laws

20 state consumer privacy laws

- Currently in effect: California, Colorado, Connecticut, Florida, Montana, Oregon, Texas, Utah, Virginia
- 2025 effective dates: Delaware, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, Tennessee
- 2026 effective dates: Indiana, Kentucky, Rhode Island

17 of those laws address AI/Automated Decision Making

- Already effective: CA, CO, CT, DE, MT, NE, NH, NJ, OR, TX
- Effective dates in July 2025 or later: IN, KY, MD, MN, RI, TN



State Consumer Privacy Laws: Rights & Obligations

- **Notice and Transparency:** What data is collected and how will it be used?
- **Control of use, disclosure, and retention of personal data**
- **Consumer Rights:**
 - Right to access
 - Right to correct
 - Right to delete
 - Right to data portability
 - Right to opt-out
 - Targeted advertising
 - Sale of personal data
 - Profiling in furtherance of a decision that produces a legal or similarly significant effect

State Consumer Privacy Laws: Rights & Obligations

- **Data protection assessments**
 - Some states require assessments prior to engaging in certain AI-driven activities that pose a “heightened risk of harm”
- **Data retention & disposal requirements**
- **Data security**



Federal Privacy Law: Current Status

Republican working group considering comprehensive framework

- DEC 2024: Congressman Brett Guthrie (KY), Chairman of House Committee on Energy & Commerce, said that his Committee would “prefer to do a comprehensive privacy bill” while at least planning to focus on finalizing children’s online safety if a comprehensive bill didn’t materialize.
- FEB 12, 2025: Guthrie launched 9-member Republican working group to explore options for a comprehensive framework.
-

Federal Privacy Law: Current Status

- Guthrie & Congressman John Joyce (PA), Vice Chairman of the Committee, issued a RFI regarding a federal privacy law.
 - Accepted input until April 7, 2025
 - Questions included
 - Role of players in data protection space (controllers, processors, third parties)
 - Should there be different treatment for companies of different sizes?
 - Scope of privacy laws – including definition of PI and SPI
 - *Scope/content of privacy disclosures*
 - *Which consumer protections should be included?*
 - *What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?*
 - Any insights learned from existing comprehensive data privacy and security laws
 - Degree to which US privacy protections are fragmented at the state-level and the costs associated with fragmentation
 - *What is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?*
 - Efficacy of existing data privacy and security laws, including “impacts on both data-driven innovation and small businesses”
 - *How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?*
 - Who should enforce the law?
 - If the FTC enforces, what resources and authorities should be made available to it?

Federal Privacy Law: Pre-Election Proposed Legislation

- The American Privacy Rights Act of 2024

- Bi-partisan consumer privacy legislation
- Would have created consumer rights similar to many state privacy laws (right to access, delete, correct, transport data; opt-out rights, etc.)
- Data minimization obligations would have been stricter than most existing state privacy laws (similar to MD)
- House subcommittee held preliminary hearings on the legislation; did not pass

- Key Features

- Data minimization requirements would have impacted development of AI by restricting the volume of datasets available to AI developers.
- Would not have pre-empted state-specific criminal laws relating to deepfakes
- Regulated “covered algorithms” (automated decision-making), defined as: *“a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision-making by using covered data, which includes determining the provision of products or services or ranking, ordering, promoting, recommending, amplifying, or similarly determining the delivery of display of information to an individual”*

Federal Privacy Law: Pre-Election Proposed Legislation Cont.

- AI developers/deployers would have been required to:
 - Conduct impact assessments
 - Provide notice & opt-out options to users if covered algorithm used for “consequential decisions” (i.e. relating to access to or equal enjoyment of housing, employment, education enrollment or opportunity, healthcare, insurance, credit, or place of public accommodation)
 - Evaluate the design of algorithms when used in interstate commerce
 - FTC would have had authority to introduce exemptions for algorithms to pose minimal/low risk
- Private right of action



Data Minimization

Maryland's consumer privacy law contains broader data minimization provisions than prior state laws:

- Data minimization similar to what was proposed in prior proposed federal legislation.
- Would require data controllers to limit data collection to what is “**reasonably necessary and proportionate to provide or maintain a product or service requested by the consumer to whom the data pertains.**”
- Processing limited to where it is “**reasonably necessary and proportionate**” in relation to identified purposes.
- Requires that collection, processing and sharing of sensitive data be reduced to what is “**strictly necessary in relation to a requested product or service.**”

AI Bias Laws -- NYC LL 144

- **What It Does:** Regulates use of Automated Employment Decision Tools (AEDTs) in hiring and promotion decisions.
- **Key Requirements:**
 - Annual **bias audit** of the tool
 - Public posting of audit results
- **Notice to candidates** at least 10 days before use
- **Why It Matters:** First law to require bias audits for AI tools in employment; noncompliance = fines.



AI Laws -- California ADT Regulations



- **What It Does:** Applies FEHA to ADTs used in employment (hiring, promotion, firing).
- **Key Features:**
 - **Disparate impact = discrimination**
 - Lack of **anti-bias testing** can be used as evidence
 - Employer must show **job-relatedness and business necessity**
- **Why It Matters:** Expands FEHA to AI tools; no safe harbor just for using a vendor.

AI Bias Laws -- Illinois Human Rights Act Amendments (Effective 2025)



- **What It Does:** Requires notice to employees/applicants of ADT use; creates liability for discriminatory outputs.
- **Key Features:**
 - Must explain what the ADT evaluates
 - Individuals can request **alternative evaluation**
- **Why It Matters:** Adds new compliance obligations for employers using any AI for screening or evaluation.

Colorado SB 24-205 (Effective 2026)

- **What It Does:** Requires AI risk management practices for “high-risk” AI systems including employment.
- **Key Requirements:**
 - Conduct **impact assessments**
 - Implement **governance and documentation**
 - Provide **notice** to individuals
- **Why It Matters:** Will be the most comprehensive state AI governance law when effective.



AI Bias Laws – Federal Guidance




- **EEOC** (Title VII & ADA)
 - Employers are liable for **discriminatory outcomes** even from vendor AI tools.
 - Must offer **reasonable accommodations** for AI tools.
- **FTC**
 - Enforces against **unfair or deceptive AI practices** (e.g., misrepresenting how AI works).
- **CFPB**
 - AI used in credit/employment decisions must allow for **adverse action explanations**.
- **DOJ/EEOC Technical Assistance (2022)**
 - Employers must ensure AI tools don't violate disability rights or discriminate based on protected class.

AI Bias Laws – EU AI Act (for Multinational Employers)

- **What It Does:** Risk-based regulation of AI systems, including employment-related tools
- **Why It Matters:** U.S. companies with EU operations or data subjects may be affected
- **Requirements:**
 - Risk classification
 - Conformity assessments
 - Transparency & human oversight for high-risk tools





PRIVACY RIGHTS & RISKS

Principles of Global Privacy Law That Apply to AI



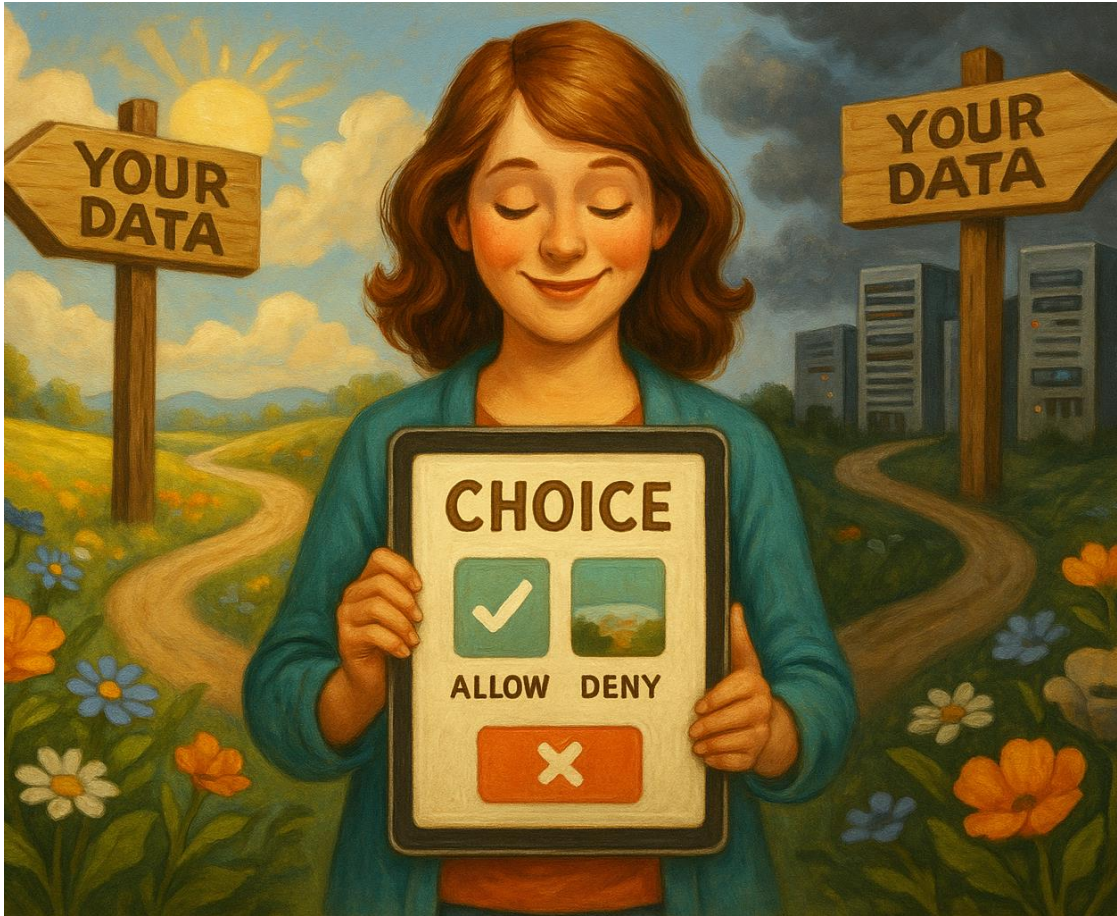
- Existing privacy and data protection principles apply to AI governance.
- Key principles include:
 - Notice
 - Choice
 - Consent
 - Purpose limitation
 - Data minimization
 - Privacy by design

Key Principles -- Notice

- Individuals should clearly understand what data is being collected and understand their rights.
- Provide information on the purposes of processing, retention periods and with whom personal information will be shared.



Key Principles -- Choice



- Individuals should be allowed to agree or disagree with the collection and use of their personal data in AI systems.

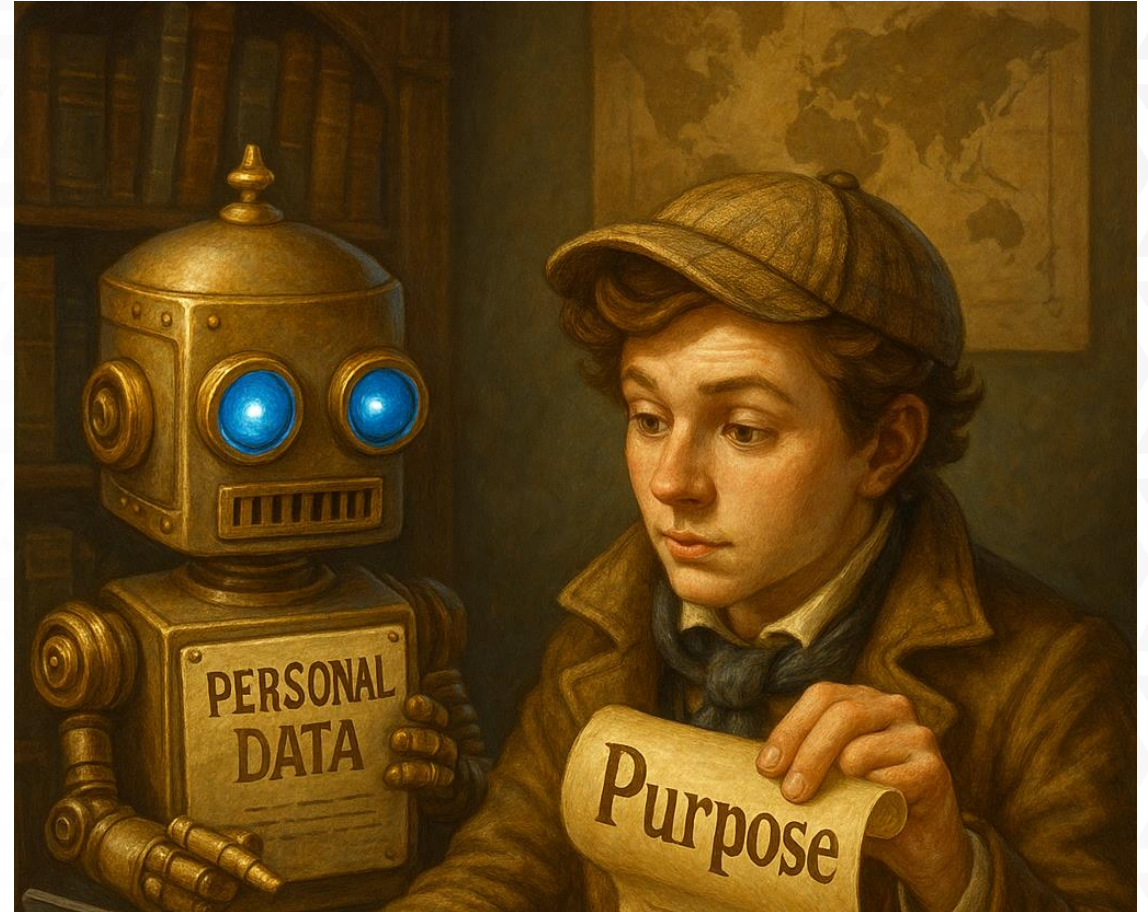
Key Principles -- Consent

- You must obtain explicit, informed and unequivocal consent from individuals to use their personal data.
- Requests for consent should be clear and concise, ensuring that individuals understand what they are agreeing to.



Key Principles -- Purpose limitation

- AI systems should collect and use personal data only for the specified purpose.
- If the use of the data changes, you should secure a new consent.



Key Principles -- Data Minimization

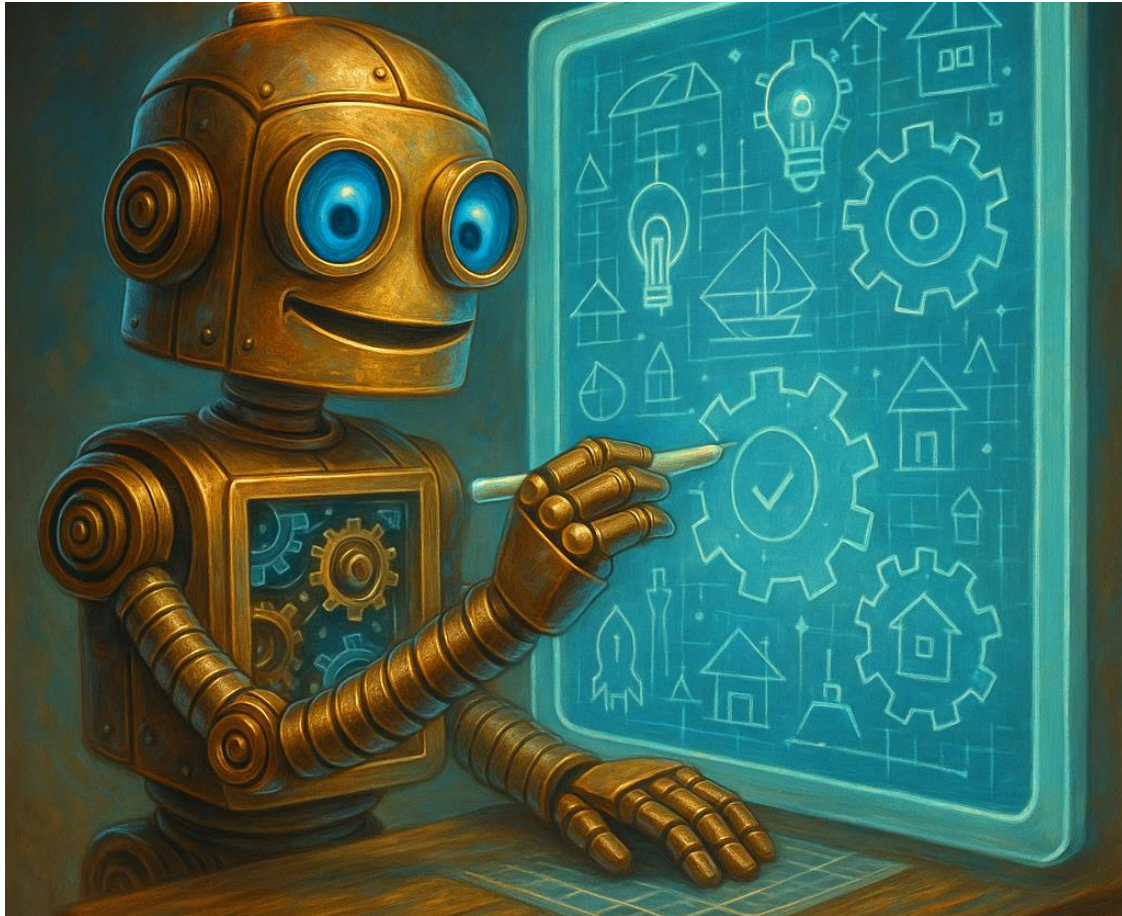
- AI systems should only collect data that is necessary for the specified purpose.
- This principle helps in reducing the amount of personal data processed, thereby minimizing potential risks to privacy.



**There is an
internal tension
between AI data
needs and data
minimization.**



Key Principles -- Privacy by Design

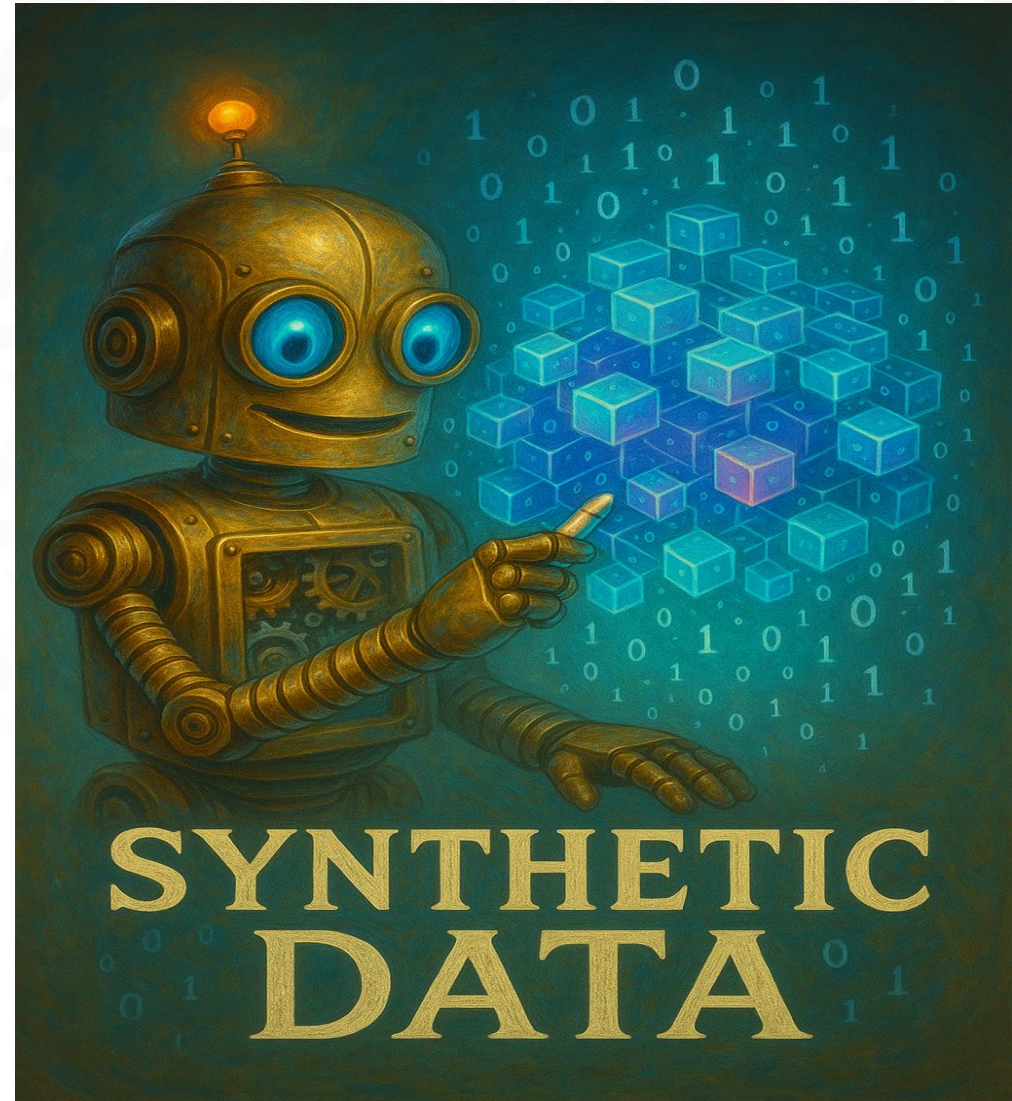


- AI systems should be designed, developed, and deployed with data protection and privacy principles applied from the beginning.
- Privacy should be “baked into” your AI applications and services.

Privacy-Enhancing Technologies (PETs)

Key technologies:

- Differential privacy
- Federated learning
- Homomorphic encryption
- Synthetic data use cases



An illustration of an office scene with a city skyline in the background. Three people (two men and one woman) are seated at desks, looking concerned. A large robot with glowing blue eyes and a white suit is seated at a desk in the foreground, looking towards the left. A computer monitor in the center displays a stylized robot head. The text "AI BIAS AND DISCRIMINATION" is overlaid in large white letters.

AI BIAS
AND

DISCRIMINATION

Avoiding AI Bias

Vet vendors for fairness testing

- Demand documentation of audits
- Ask about their training data

Conduct internal validation

- Test outputs using your workforce data
- Apply multiple fairness metrics

Disclose AI use to applicants/employees

- Clear notices before use
- Offer alternative assessments or accommodations



Avoiding AI Bias

Avoid over-reliance

- Use AI as a *decision-support tool*, not a final decision-maker
- Retain human oversight

Document everything

- Why a tool was chosen
- Records of internal testing and review
- Employee complaints or challenges



AI SECURITY RISKS



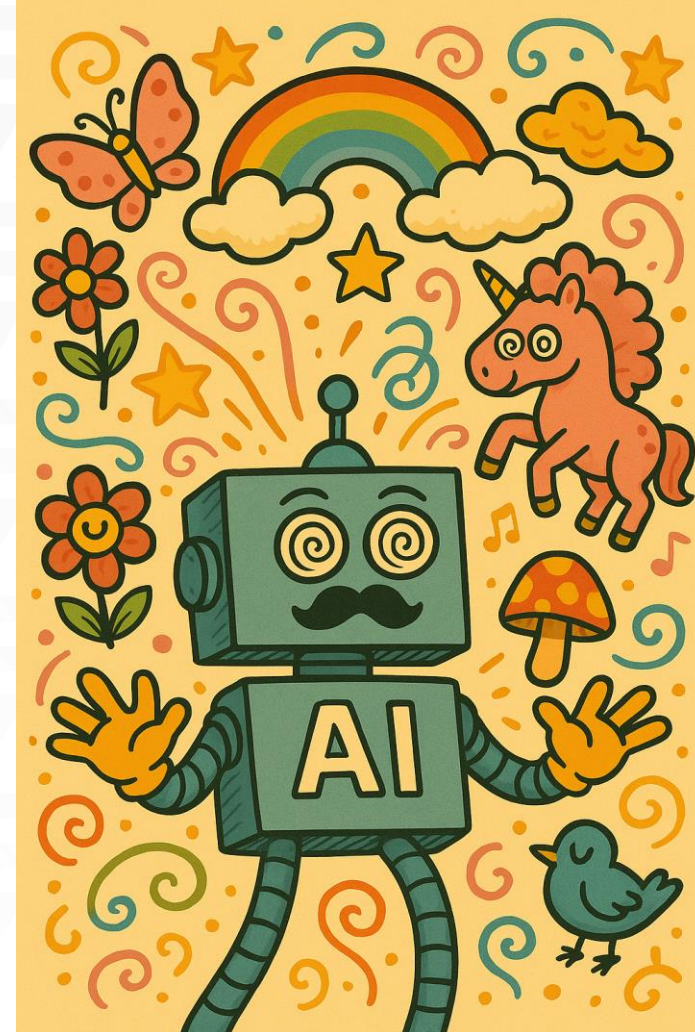
Security risks from Gen AI

- Hallucinations
- Deepfakes
- Data Leakage
- Filter Bubbles/Echo Chambers
- Shadow AI



Gen AI Risks -- Hallucinations

- Gen AI models are probabilistic
- Prone to generate wrong or fake answers (but won't tell you they're potentially fake)
- Newer models like GPT-4, Claude 3, and Gemini 1.5 have significantly reduced hallucination rates.



Gen AI Risks -- Deepfakes



- Deepfakes are really, really good imitations.
- Videos, audio, photos, text messages, and other forms of media created using AI that are extremely hard to differentiate from the real or authentic thing
- In June 2022, the FBI issued a warning that deepfakes were being used in remote job interviews.

Deepfake Video Scam

- A finance worker at a multinational firm was tricked into paying out \$25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call.
- The scam involved a phishing email sent from the firm's CFO asking for a secret transaction.
- Although the employee was suspicious, he believed everyone else on the call was real.
- The employee sent a total of \$200 million Hong Kong dollars – about \$25.6 million – to the scammers.



Emerging Threats

FORTUNE

Thousands of North Korean IT workers have infiltrated the Fortune 500—and they keep getting hired for more jobs

Amanda Gerut
Mon, April 7, 2025 at 7:00 AM EDT · 9 min read

1.1k

Firm hacked after accidentally hiring North Korean cyber criminal

16 October 2024

Share Sav

WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE

MATT BURGESS SECURITY MAY 14, 2025 6:00 AM

North Korean IT Workers Are Being Exposed on a Massive Scale

Security researchers are publishing 1,000 email addresses they claim are linked to North Korean IT worker scams that infiltrated Western companies—along with photos of men allegedly involved in the schemes.

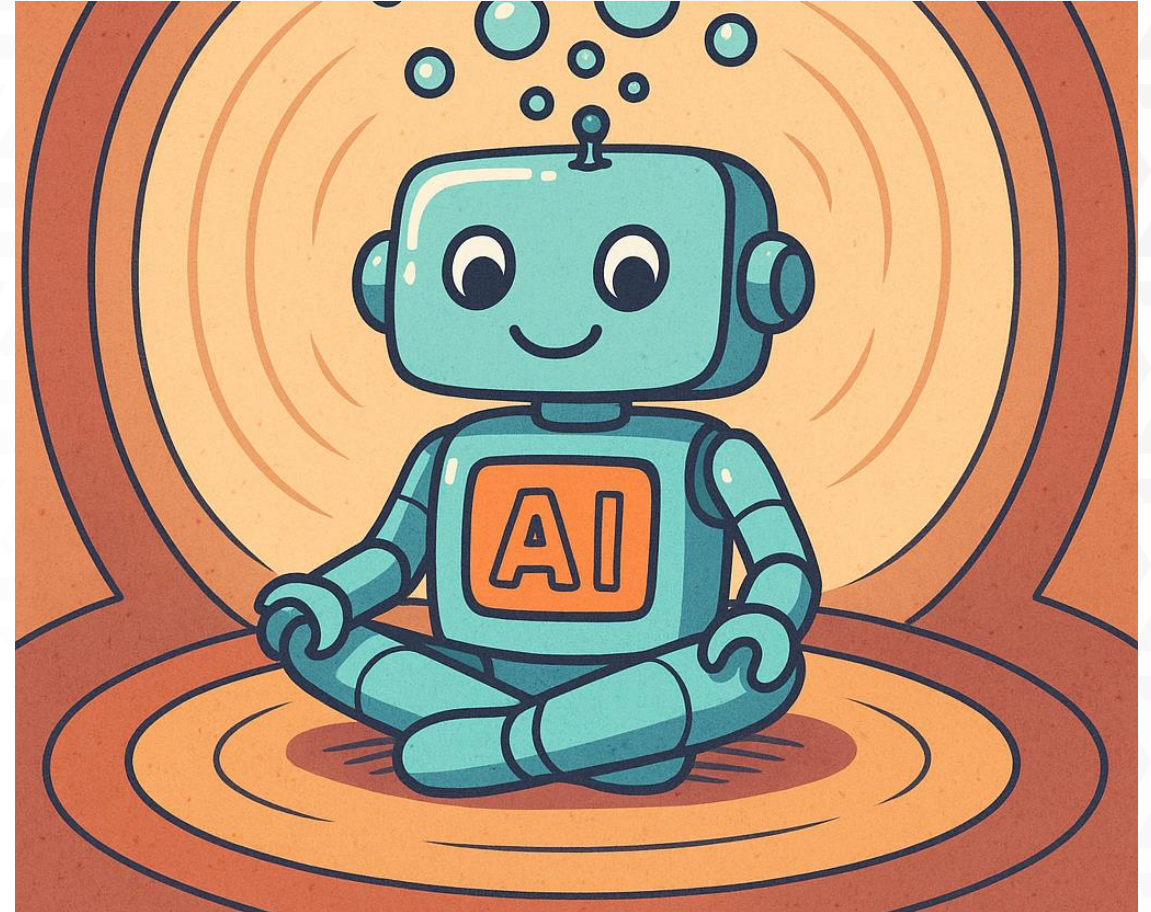
Gen AI Risks -- Data Leakage

- Unauthorized disclosure of data to a third party.
- This happens in almost all data projects.



Gen AI Risks – Filter Bubbles/Echo Chambers

- No new insights or information
- Gen AI repeats back to the user what they already believe or have told the AI system



Shadow AI



- Employee “covert” use of Gen AI tools
- 75% of global knowledge workers reported using AI at work, with 46% having started within the previous six months
- 57% keep this use hidden
- Adopt clear Acceptable Use policy (minimum), training, BYOAI, monitor usage

AI Model Security Risks

- **Model inversion attacks** aim to reconstruct sensitive training data or extract details about individual data entries from an AI model's outputs.
- This type of attack exploits the model's ability to provide detailed outputs to reverse-engineer or infer information about the input data, potentially compromising data privacy.
- It is especially concerning when models handle sensitive personal data, like in healthcare or financial services.



AI Model Security Risks

Model extraction, also known as model stealing, occurs when an adversary attempts to create a nearly equivalent model by systematically querying an AI system and observing its responses.



AI Model Security Risks



Model poisoning refers to the intentional manipulation of an AI model's training data or learning environment to induce specific errors in output.

This can happen during the data collection or training phase when an attacker injects malicious data into the training set.

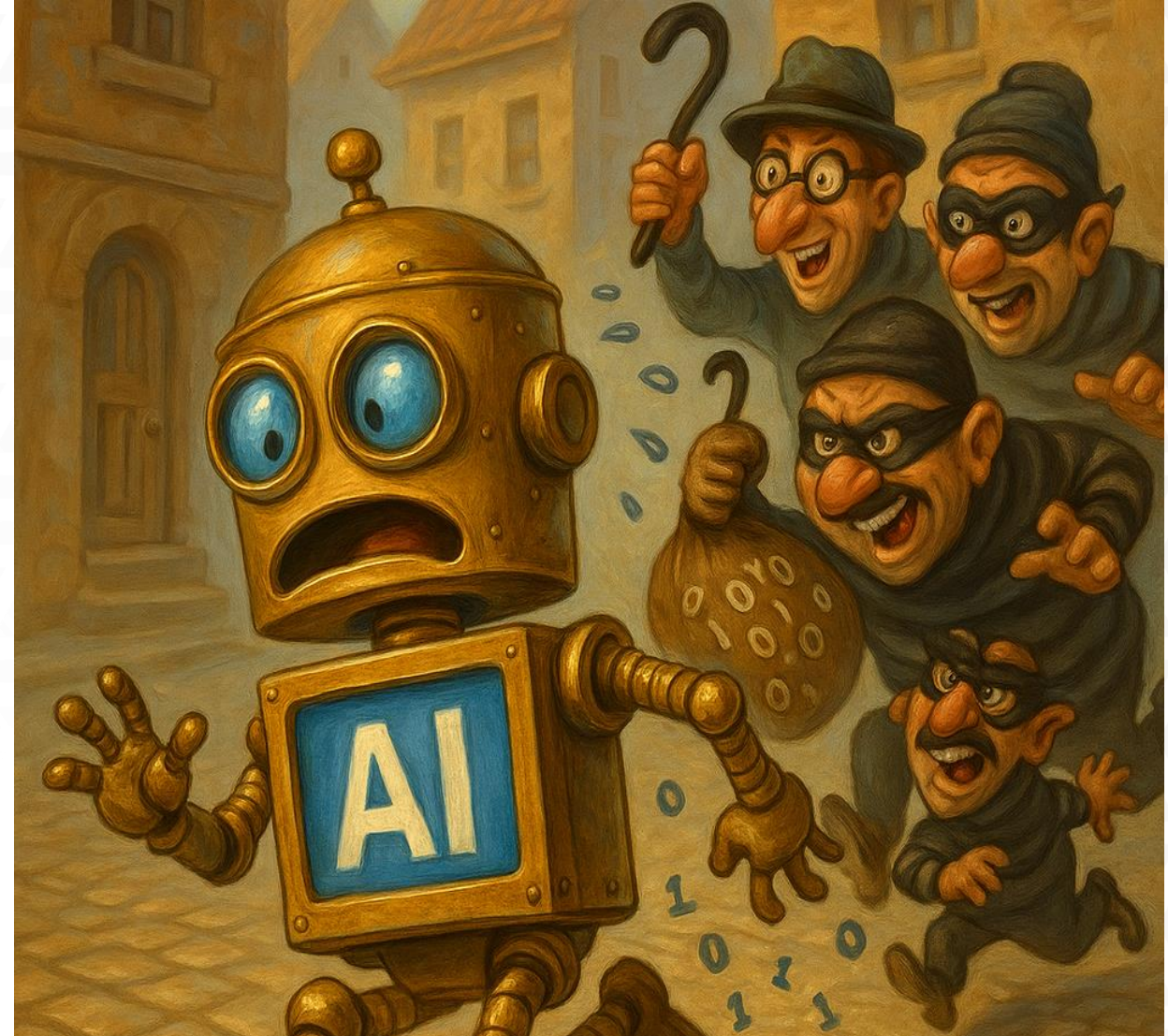
This causes the model to learn incorrect patterns and make faulty decisions.

AI Security Risks

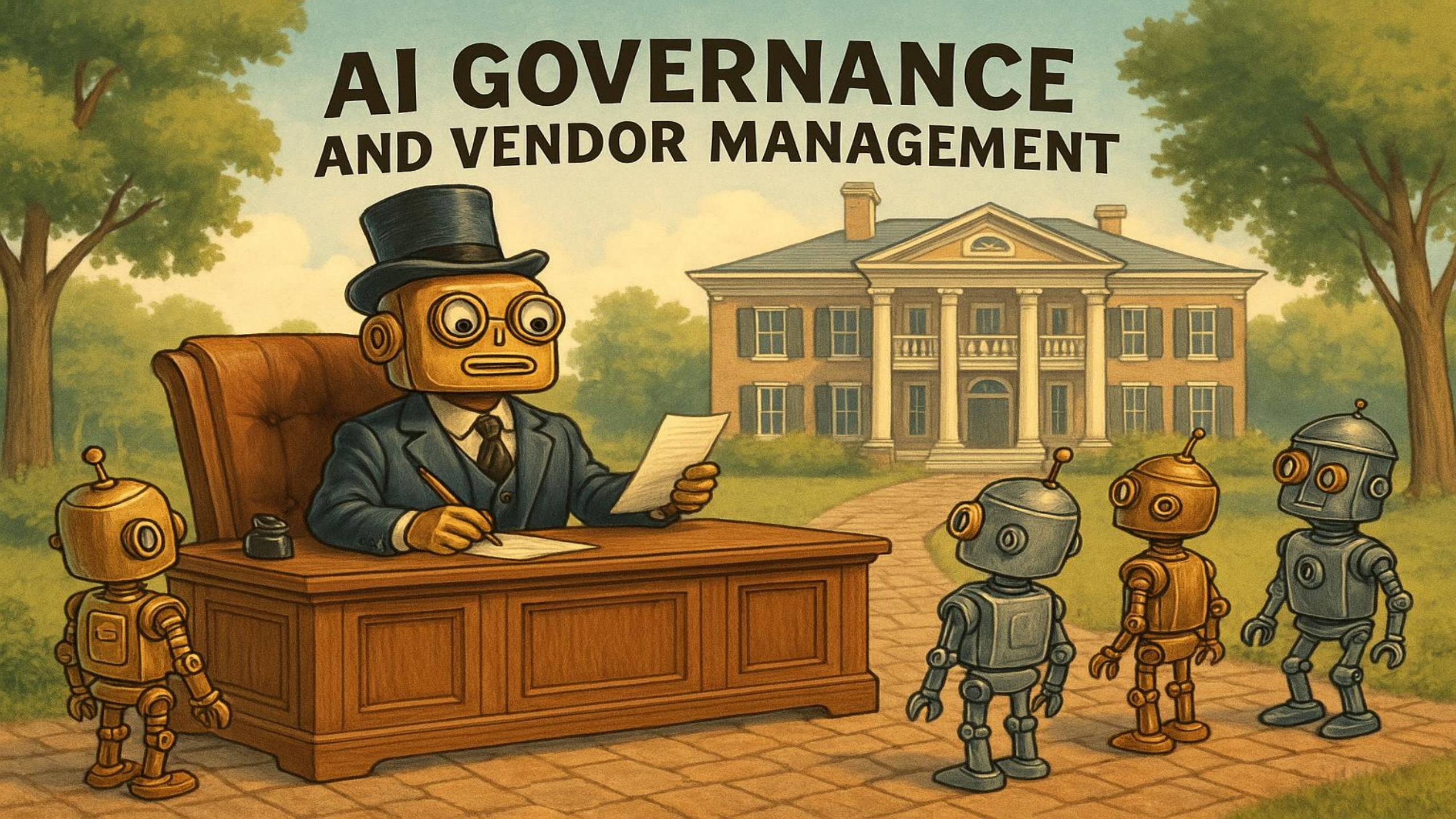
Model evasion, often linked with adversarial attacks, involves crafting inputs that are designed to deceive AI models into making incorrect decisions.

Typically slight modifications of legitimate data that cause the model to misclassify or mispredict, all while appearing normal to human observers.

Evasion attacks are particularly dangerous as they can be used to circumvent systems that rely on AI for critical decision-making, such as security systems or fraud detection.



AI GOVERNANCE AND VENDOR MANAGEMENT



What is AI Governance?

- A system or framework that helps companies monitor or manage their AI-related activities.



Steps for Building AI Governance

- Threshold Questions:
 - Are you a user, a developer, or both?
 - Why did you believe you need AI Governance – who should you protect – employees, end users, company, shareholders, reputation, vendors, customers?
 - What, if any, governance program do you already have in place?
 - What policies does your company currently have in place that touch on AI (e.g., privacy)



Why the NIST AI RMF Matters



Developed by NIST to:

- Align AI use with organizational values and risk tolerance
- Support trustworthy AI deployment in real-world settings
- Help businesses and agencies meet growing regulatory expectations

The 4 Core Functions:

- **Govern** – Risk culture, policies, and oversight
- **Map** – Know your AI: its purpose, context, and risks
- **Measure** – Analyze how well it performs and where it fails
- **Manage** – Act on risks with meaningful controls

Keys to Governance



**Build a
Process**



**Follow
the Process**



**Document
the Process**

Practical Tips for AI users to comply with privacy laws



Practical Tips

- Conduct PIAs and DPIAs prior to making AI tools available for public use.
- Have a system in place for human oversight and for review of AI input and output.
- After deployment, the assessments must be regularly conducted.
- Provide transparent information on personal data collection and usage; share information on privacy risks with deployers; ask your vendors for their risk process, risk assessments, and mitigation efforts.
- Develop data retention and deletion plans for any personal information collected; conduct training on data destruction and deletion policies; audit compliance.
- Implement cybersecurity controls and prevention techniques to keep attackers from extracting personal data from AI systems; check your vendors cybersecurity measures.

AI Advantage: An FP Conference for Business Leaders



fpSolutions – AI



QUESTIONS?



THANKS

For Joining Fisher Phillips



David J. Walton, AIGP, CIPP/US

Partner | Philadelphia

dwalton@fisherphillips.com

610.230.6105



Risa B. Boerner, CIPP/US, CIPM

Partner | Philadelphia

rboerner@fisherphillips.com

610.230.2132

**Fisher
Phillips**