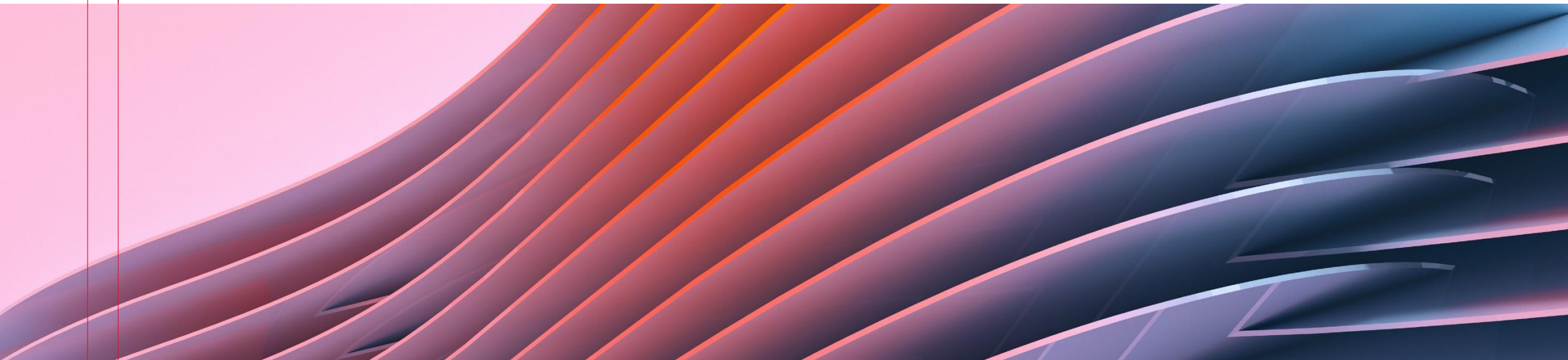
Kilpatrick | ACC Association of Corporate Counsel DALLAS-FORT WORTH

Data Risk in 2026: The Privacy Challenges Corporate Counsel Can't Ignore



Today's Agenda

1. Emerging Privacy
2. AI Privacy Issues
3. Data as IP
4. Consumer Notice and Choice

Objectives

- Enable attendees to spot and triage data protection risks
- Discuss best practices, compliance strategies, and governance

Privacy in a Flash

01

Emerging Risks

- **Data Monetization and Third-Party Sharing**
  - Sharing data with marketing partners, loyalty programs, ad networks
  - CCPA/CPRA "sale"/"sharing" implications and consumer rights (e.g., CPPA enforcement action based on marketing cooperatives)
  - GPC requirements continue to evolve (enforcement focus)
  - Shine the Light re-emerges
- **Children and Teen Data; Sensitive Data Generally**
  - New laws taking effect; FTC focusing on statutory based enforcement
  - State law enforcement usually involves the misuse of sensitive data (like geolocation or heath-related data)
- **AI and Automated Decision-Making**
  - Profiling, targeted advertising, and consumer risk scoring
  - New CCPA regulations

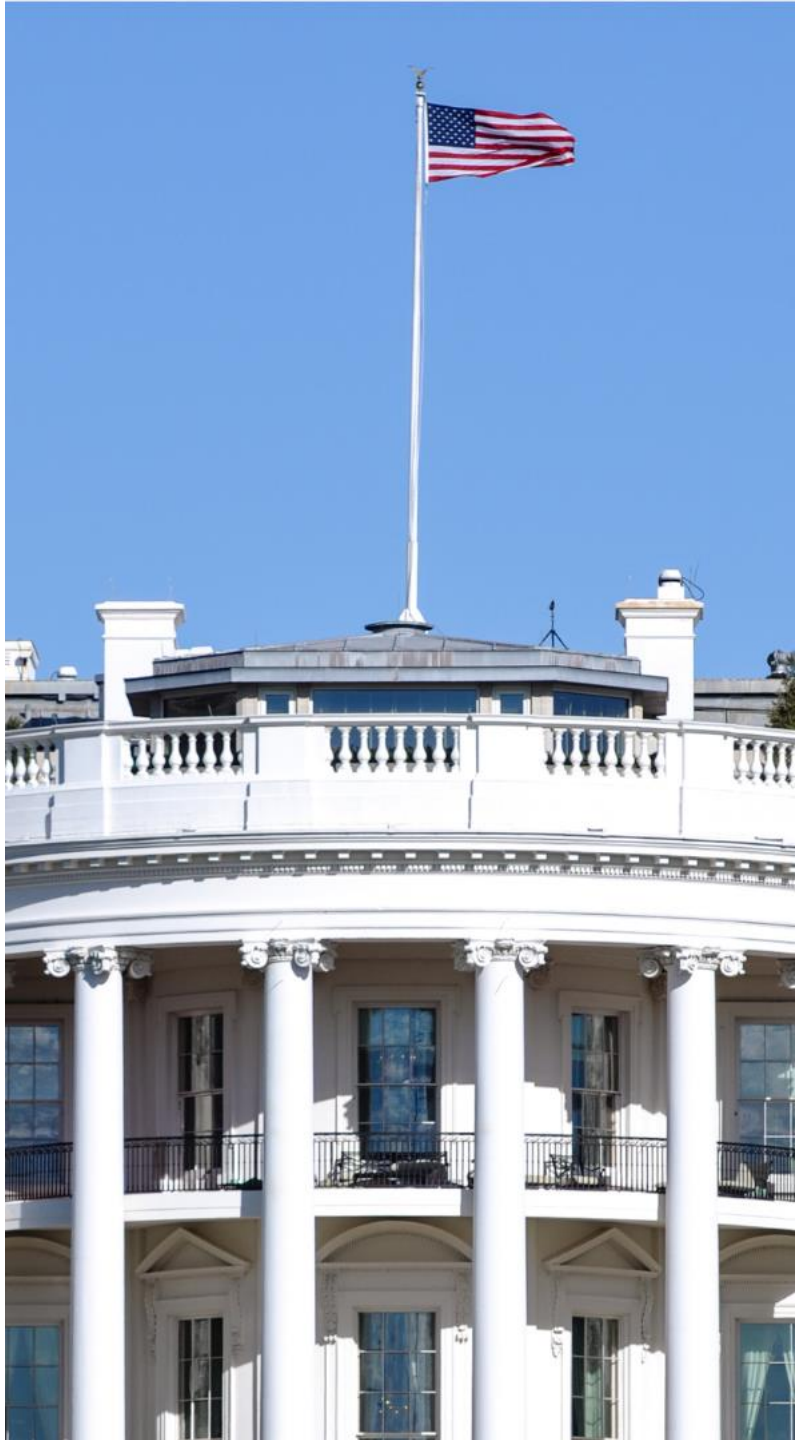
Online Tracking Litigation Theories & Developments

- **Wiretap and Eavesdropping Statutes**
  - Claims under federal and state laws (CA, FL, and PA are the most active).
  - **Allegations:** Use of session replay, chatbots, or analytics tools as "interception" of communications.
  - **Key cases:** *Popa v. Harriet Carter Gifts, Javier v. Assurance IQ*.
- **VPPA**
  - Claims against sites using video content and Meta Pixel/other trackers.
  - "Consumer" and "personally identifiable information" interpretations (current Supreme Court review)
- **Location tracking (e.g., mobile apps)**
- **Other theories**
  - Common law invasion of privacy.
  - State consumer protection statutes (UDAP).

Other Considerations

Executive Order 14117

- **Issued:** February 28, 2024; currently enforceable
- **Key Points**
  - Applies to companies sharing *bulk sensitive personal data* or *government-related data*
  - Types of agreements: vendor, employment, and investment agreements
  - Prohibits data transfers and other restricted transactions to certain countries of concern/foreign entities
  - Countries of concern: China (including Hong Kong and Macao), Cuba, Iran, North Korea, Russia and Venezuela
- **Risk Implications**
  - Conduct vendor diligence on foreign ownership/control
  - Include flow-down clauses limiting onward transfer of data
  - Marketing pixels are implicated as a form of sharing (e.g., TikTok pixel)



VENDOR MANAGEMENT

EO 14117 & Security

- **Next steps**
  - Map compliance
  - Update agreements with vendors that receive covered data
- **Organizational requirements** for covered systems that interact with covered data
  - Document and maintain inventory of assets of covered systems
  - Document and maintain vendor agreements for covered systems
  - Remediate known vulnerabilities within 45 day
  - Implement logical and physical access controls
- **Data-level requirements** for restricted transactions
  - Implement data minimization and data masking strategies
  - Apply encryption techniques to protect covered data during the covered transaction; Apply PETs to process covered data

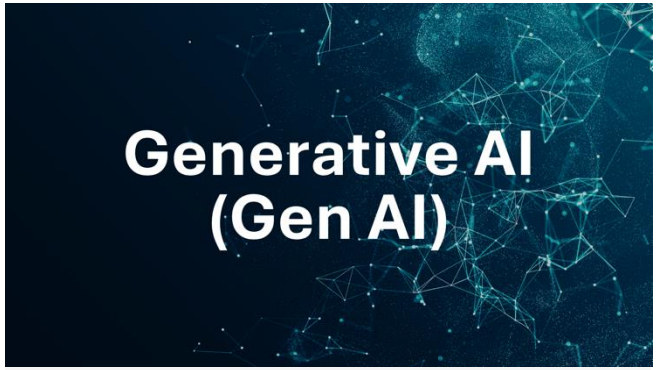
AI-Privacy Issues

02

Artificial Intelligence

Learns patterns from historical data to make predictions or classifications (e.g., "fraud" vs. "legitimate" transaction).

Operates only when triggered by data inputs or scheduled runs; does not initiate tasks or adapt strategies on its own.



Generates new, synthetic content (e.g., text, images, synthetic data) that resembles or extrapolates from training data.

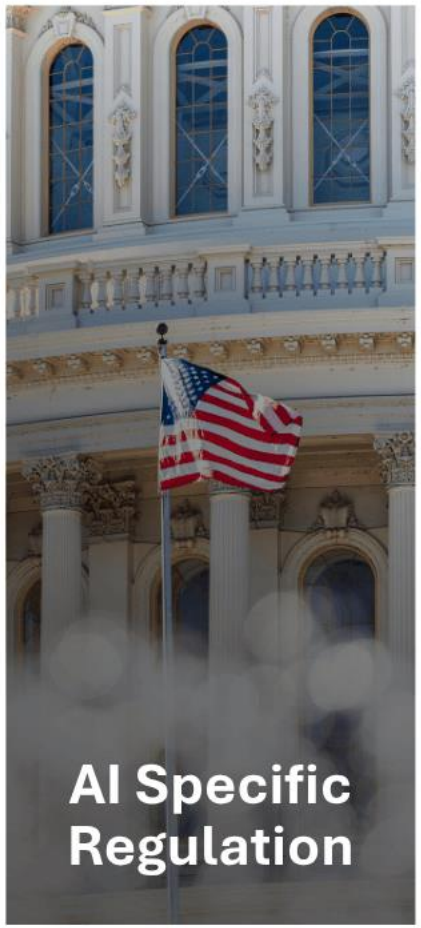
Responds to prompts with creative outputs, but does not independently monitor, act, or orchestrate multi-step processes.

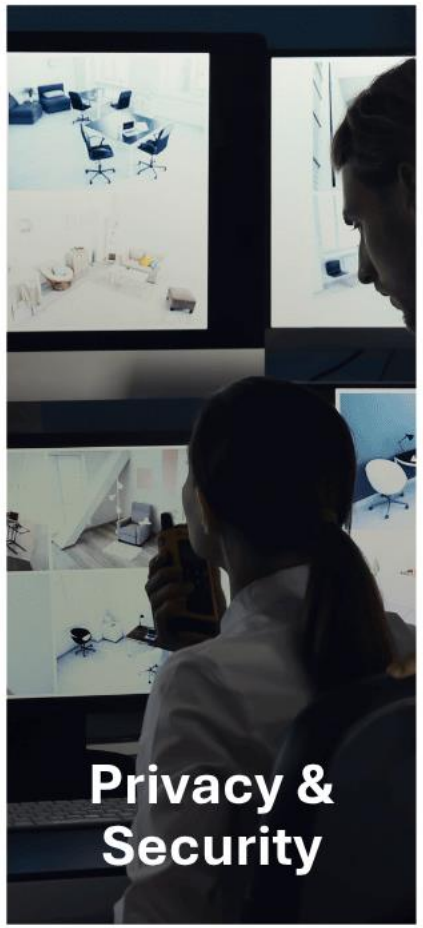
Acts autonomously toward goals, making ongoing decisions and adapting strategies in real time (persistent, goal-driven behavior).

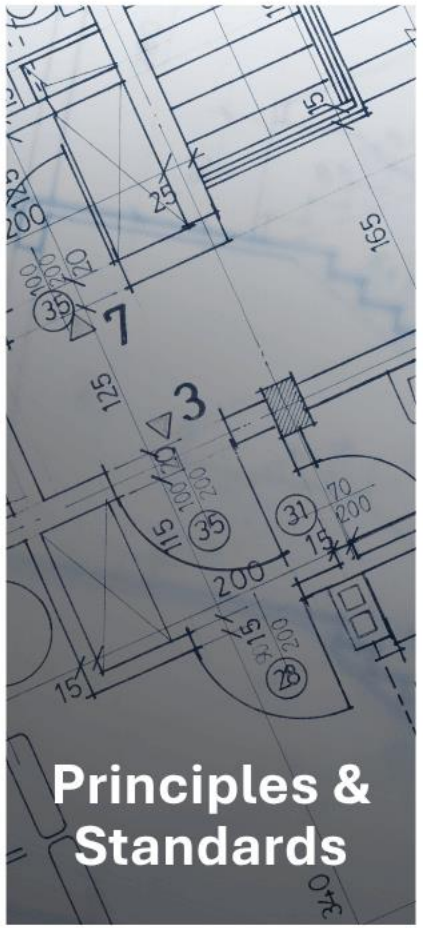
Can autonomously sequence and execute multi-step actions, collaborate across systems, and self-improve without explicit human prompting.

REGULATORY LANDSCAPE

AI Regulatory Landscape







REGULATORY LANDSCAPE

AI Specific Regulation

AI Specific (sampling)

- Colorado AI Act (eff. 6/30/26)
- CA AI Transparency Act (eff. 1/1/26)
- Utah Transparency Law (eff. 5/1/24)

AI in Employment (sampling)

- NY Local Law 144
- Illinois AI Video Interview Act
- Illinois Human Rights Act (HB 3773)

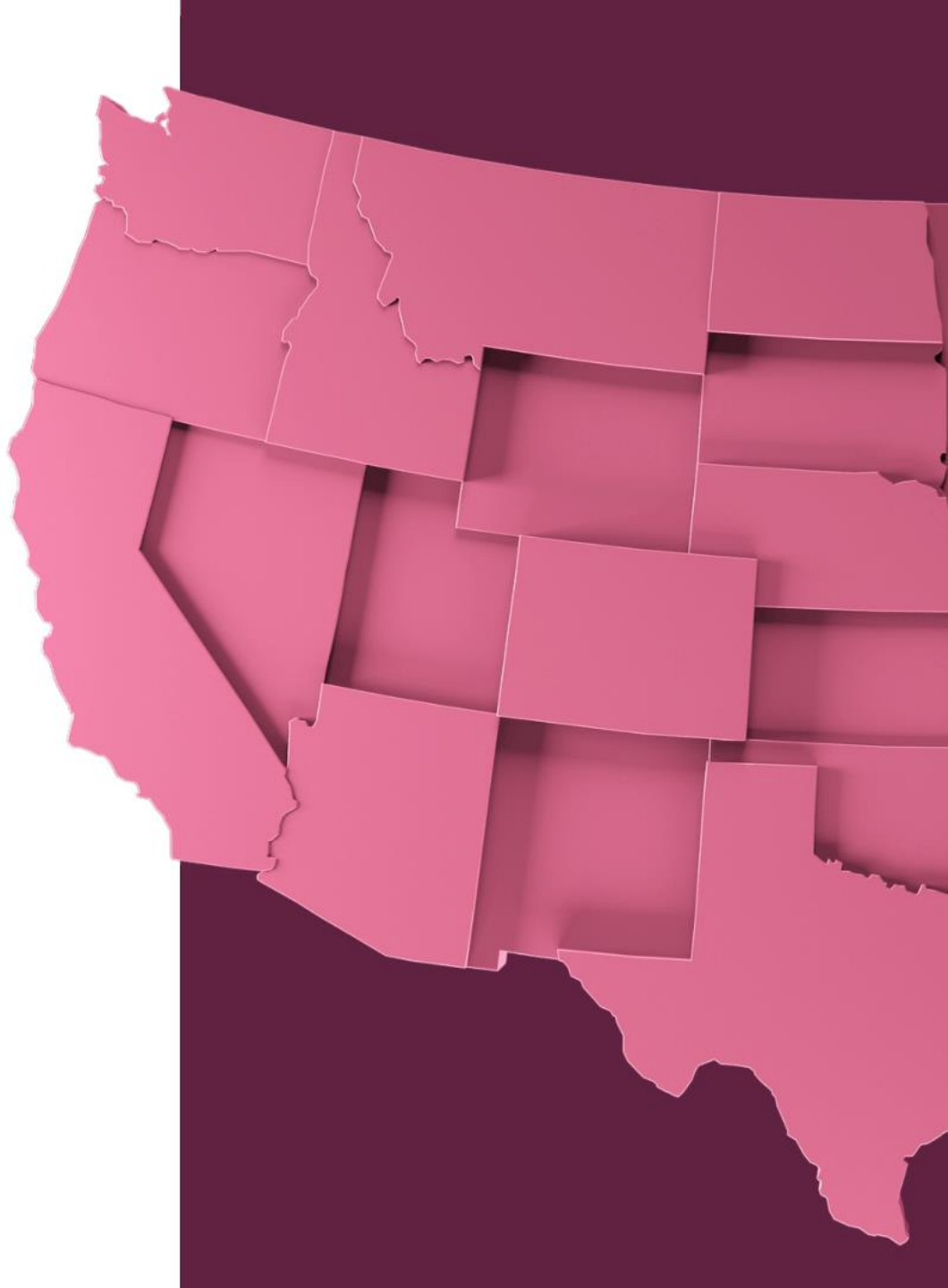
AI in the Future

- Many states have bills that are making their way through the legislative process

REGULATORY LANDSCAPE AND BEST PRACTICES

State Regulation of AI

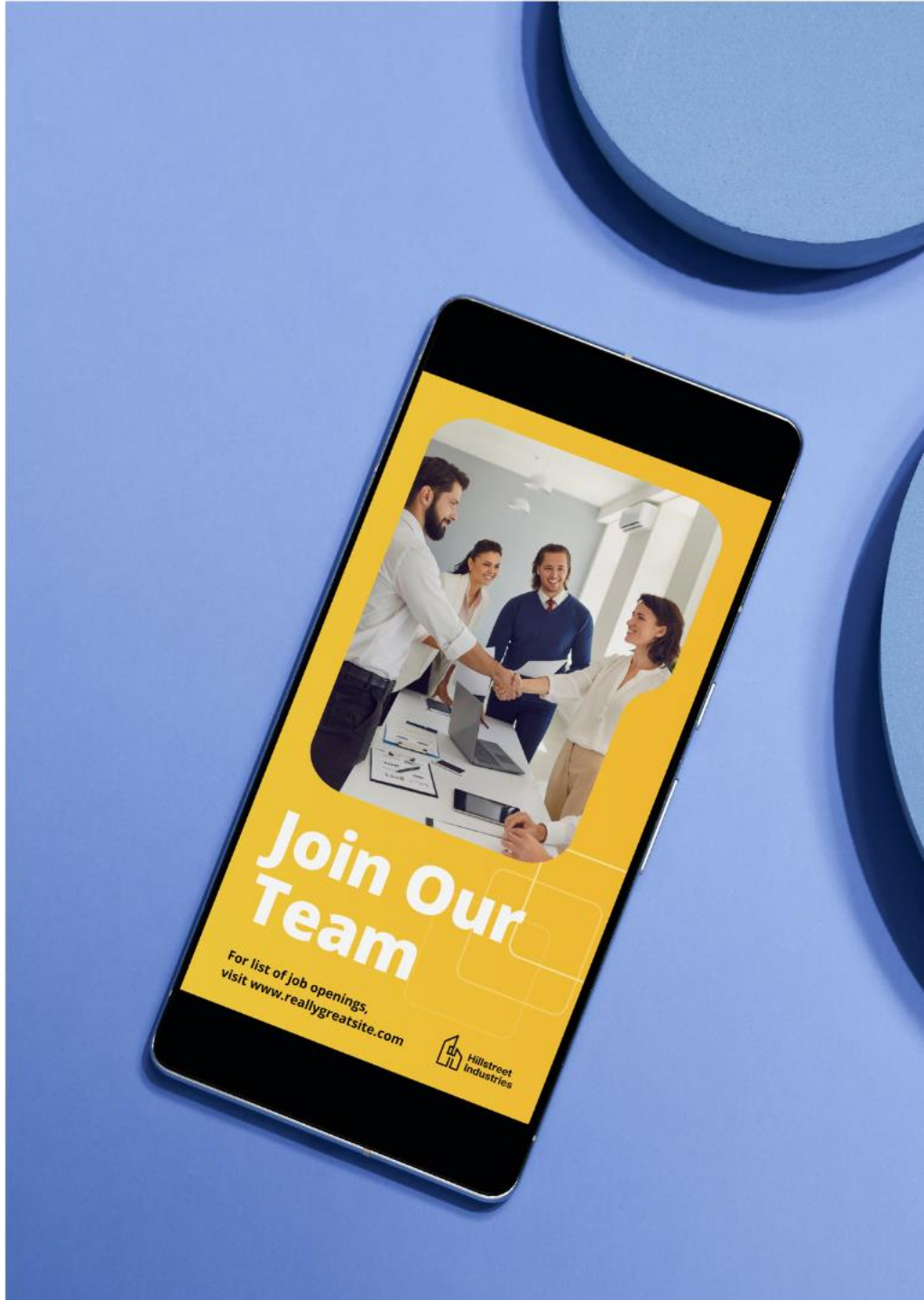
- Focus on High-Impact Use
- Preventing Discrimination
- Role-Based Obligations
- Consumer Rights Protections
- Targeted Tech Regulation



EMPLOYEE PRIVACY

How AI is Transforming HR

- AI-powered recruitment, screening, and performance evaluations
- Predictive analytics for turnover, productivity, workplace safety
- Monitoring employee communications, sentiment analysis
- Employee Avatars
- These tools process sensitive personal data
  - Risk of discrimination, bias, profiling, and non-transparent decisions
  - May fall under “automated decision-making” restrictions in CCPA, GDPR



EMPLOYEE PRIVACY

Legal Risks of AI Use in HR

- **Transparency & Notice:** Is the employee aware AI is being used? Have they consented to its use?
- **Bias & Discrimination:** Is the tool fair and explainable?
- **Data Governance:** What data is being collected, for what purpose, and for how long?
- **Data Minimization and Purpose Limitation:** Is more data being collected than the business needs?

Emerging laws: NYC's AI audit law, EU AI Act, FTC scrutiny

EMERGING RISKS

AI Risk in the Wild

Phishing & Scam

The Guardian

CEO of world's biggest ad firm targeted by deepfake scam

Exclusive: fraudsters impersonated WPP's CEO using a fake WhatsApp account, a voice clone and YouTube footage used in a virtual meet

Nick Robins-Early

Fri 10 May 2024 08.01 BST

Malware

Disinformation

BBC

Trump supporters target black voters with faked AI images

4 March 2024

Societal issues

The Guardian

Mother says AI chatbot led her son to kill himself in lawsuit against its maker

Megan Garcia said Sewell, 14, used Character.ai obsessively before his death and alleges negligence and wrongful death

Hallucinations

BBC

Apple suspends error-strewn AI generated news alerts

Privacy & legal issues

NEW YORK POST

AI is spying on your workplace gossip and secrets — and sharing them afterward

How Does This Differ From a Cybersecurity Incident?

Dimension	Cybersecurity Incident	AI Incident
Core Focus	Confidentiality, Integrity, Availability (CIA) of information assets	Socio-technical harms spanning safety, fairness, privacy, misinformation, autonomy, and physical impacts
Primary Threat	External adversary exploiting technical vulnerabilities	Can arise from model design, data, deployment context, user misuse, or malicious attack
Failure Mode	Exploit or breach of a security control or vulnerability.	Model misspecification, drift, hallucination, bias, reward hacking, adversarial attack, or security breach
Lifecycle Stage	Mostly operational / post-deployment	Pre-deployment (training data, model design), deployment, and post-deployment
Regulation	Data-protection, breach-notification, critical-infrastructure laws	Emerging AI-specific regimes plus sectoral safety, privacy, consumer protection, and antidiscrimination laws

Data as “IP”

03

Data as IP: What is Data?

Data = pieces of digital information

Database = collections of data

Sources of Data

- Data input or uploaded into the digital product
- Data collected by or derived from usage of the digital product
- Data outputs (e.g., reports, analyze, calculations, generated content, data models, etc.)
- Data/content as “the product”
- Public sources/open-source models

Categories of Data

- Raw data vs curated data
- Individual data elements vs a data collection
- Unstructured data vs. Structured data

Is Data Protectable as IP?

Copyright protection is limited

- Raw facts are not protectable
- Only creative compilations may qualify
- Fair use and text/data mining exceptions vary by jurisdiction

Trade secret law offers stronger protection

- Must show commercial value and reasonable secrecy measures
- Risk of loss if data is disclosed or poorly managed

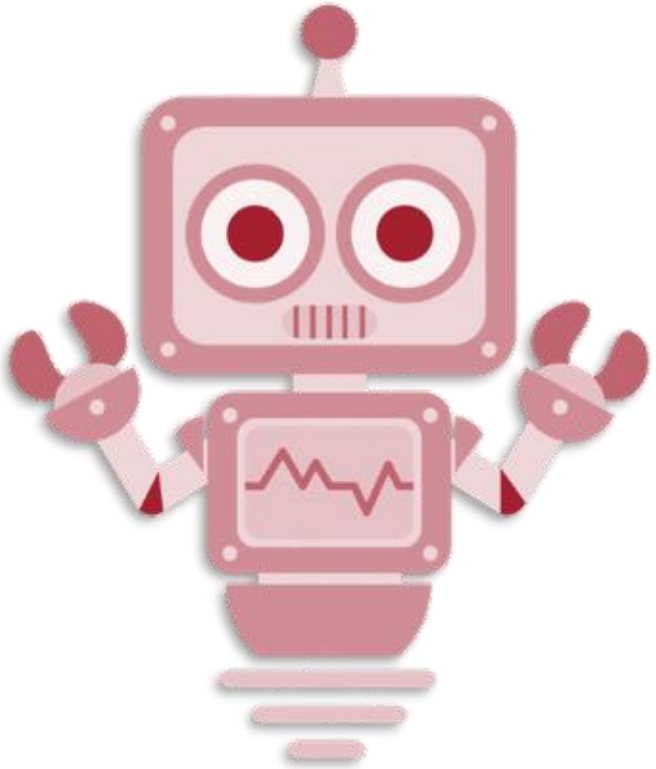
Contracts are critical

- Most data misuse comes from insiders or authorized users
- Use NDAs, vendor agreements, and terms of use to bind access

BONUS CONTENT:

Data/IP Ownership - AI

- “Input Data” and “Output Data”
- Ability to use customer data to train AI models
- Aggregated Data versus Model Training Prohibitions
- Who owns Materials developed by AI?



Negotiating Privacy Terms

Clause	Best Practice
Data Use Obligations and Restrictions	Limit to specified purposes; no vendor secondary use
Controller-Processor Roles	Subprocessor prior notice and approval; flow down obligations
Audit Rights	Risk-based audits; frequency
Breach Notification and Response	Define timelines; method of notice
Termination Procedures	Ensure data return/deletion

Other Negotiated Terms – beyond mutual compliance; vendor use rights; liability caps and indemnities; consent obligations

VENDOR MANAGEMENT

Contracting for Products with Built-In AI

- Require disclosure of AI capabilities, data sources, and decision-making.
- Define what data is used to train AI, and whether your data may be used to improve the product for others.
  - Consider banning or restricting training on your data.
- Determine who owns the outputs.
- Limit liability for AI-driven errors.
- Require compliance with applicable regulations (EU AI Act, NIST AI Framework).
- Reserve the right to review AI systems and conduct impact assessments.

Consumer Notice and Consent

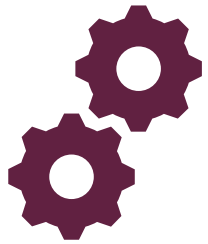
04

Consumer Notice & Consent

Notice

Consent

Opt-In/Opt-Out

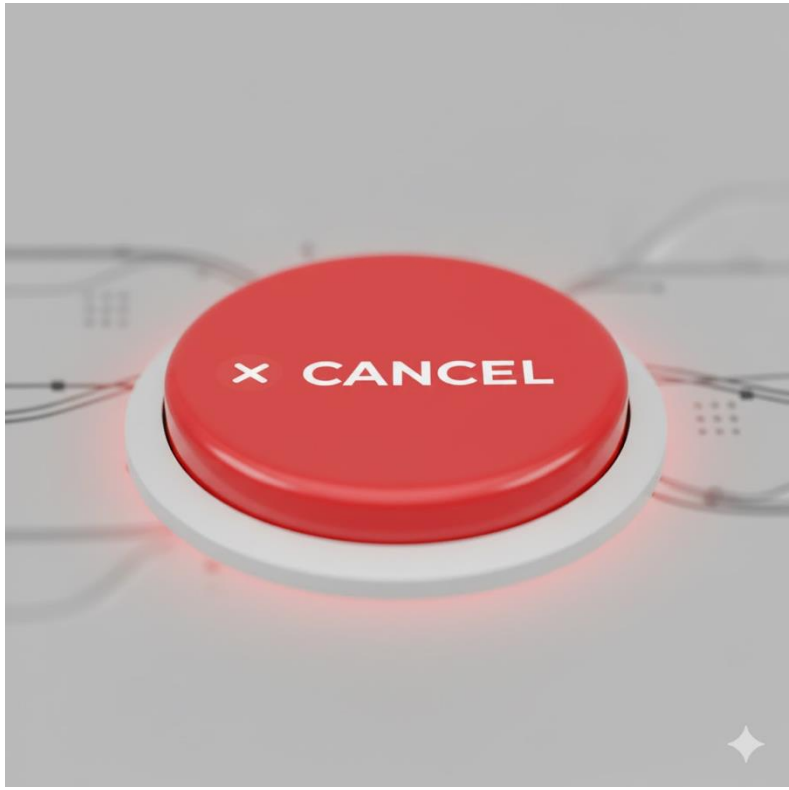


User Controls

- **Consumer "notice" vs. Consumer "consent"**
  - Transparency about data practices vs. user agreement
- **"Opt-out" vs. "opt-in" Consent requirements**
  - User control over participation
- **Obtaining Consent**
  - How is user consent obtained for data collection and processing?
- **User Rights & Controls**
  - Are there mechanisms for users to opt-out or manage their privacy preferences?
  - Can users access, modify, or delete their data?

Consumer Notice & Consent

Issue	Business Activity	Legal Risks Focus
Subscription & Auto-Renewal	**"Click-to-Cancel" Mandates:** Companies make it easy to sign up online but difficult to cancel (e.g., forcing phone calls, complex menus, or "churn surveys").	State laws and proposed rule require cancellation to be **as simple as enrollment.**
Hidden Fees	Not disclosing the full price, including mandatory charges, until the last step of a transaction.	The FTC is actively targeting **misleading price displays** and other forms of deceptive design.
AI Washing	Making false claims about a digital service's features or quality.	**False advertising** claims and FTC or state AG enforcement based on unfair or deceptive practices
Algorithmic Pricing	Using proprietary data and algorithms to create non-credit scores that lead to **differential pricing**.	**Notice** (NY laws) and other regulatory considerations (e.g., unfairness and price fixing issues)



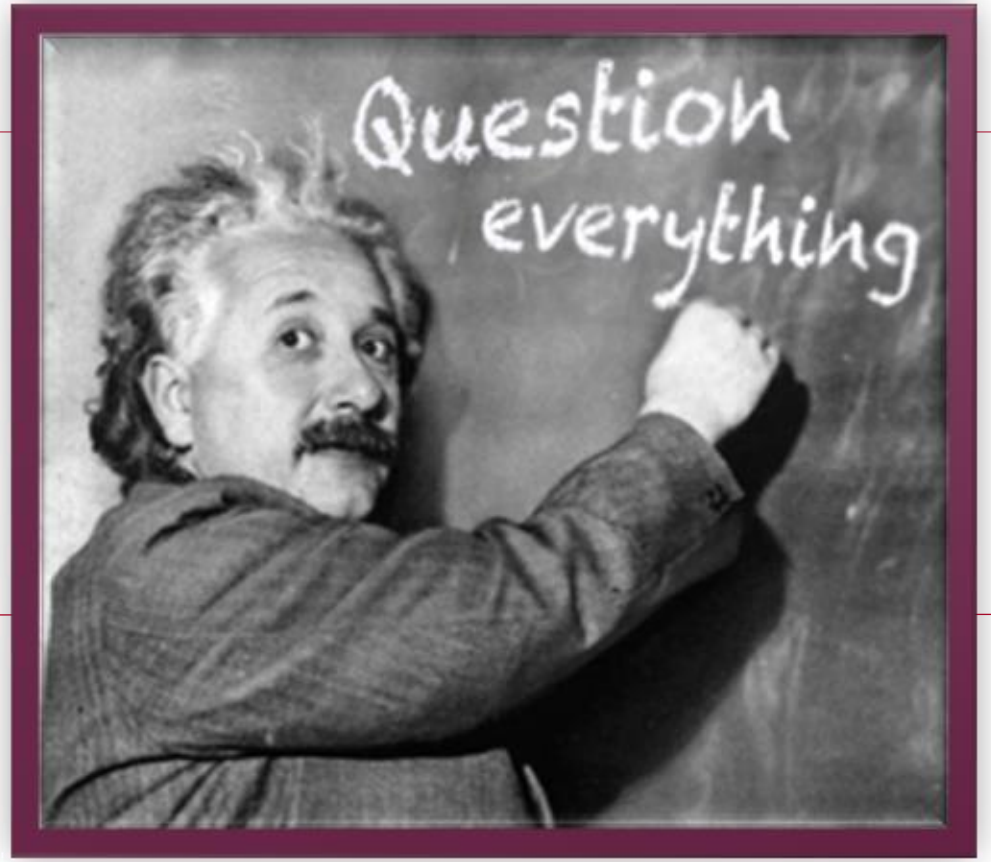
Presenter

John Brigagliano
Partner

Atlanta

404 541 6816
jbrigagliano@ktslaw.com

Questions?



Kilpatrick

ktslaw.com

Anchorage | Atlanta | Augusta | Beijing | Charlotte | Chicago | Dallas | Denver | Houston | Los Angeles New York | Phoenix | Raleigh | San Diego | San Francisco | Seattle | Shanghai | Silicon Valley Stockholm | Tokyo | Walnut Creek | Washington D.C. | Winston-Salem