Buchalter

www.buchalter.com

Avoiding Bingo – 2026: Practical Guidance on Technology Risk Management

Stephanie Wilkins, CIPP/US, CIPM
Special Counsel – Salt Lake City
Data Protection and Privacy

Daniel A. Pietragallo, AIGP, CIPP/US, FIP
Special Counsel - Denver
Co-chair of AI Governance Group

Jason W. Croft
Partner – San Francisco, Salt Lake City
Global Chair of Patent Procurement and Strategy

ACC MountainWest Techlaw Symposium, March 27, 2026

State Attorneys General Do Not Need AI Laws to Regulate

February 25, 2026

MEMORANDUM TO ALL STATE OFFICIALS, AGENCIES, AND CONCERNED PARTIES

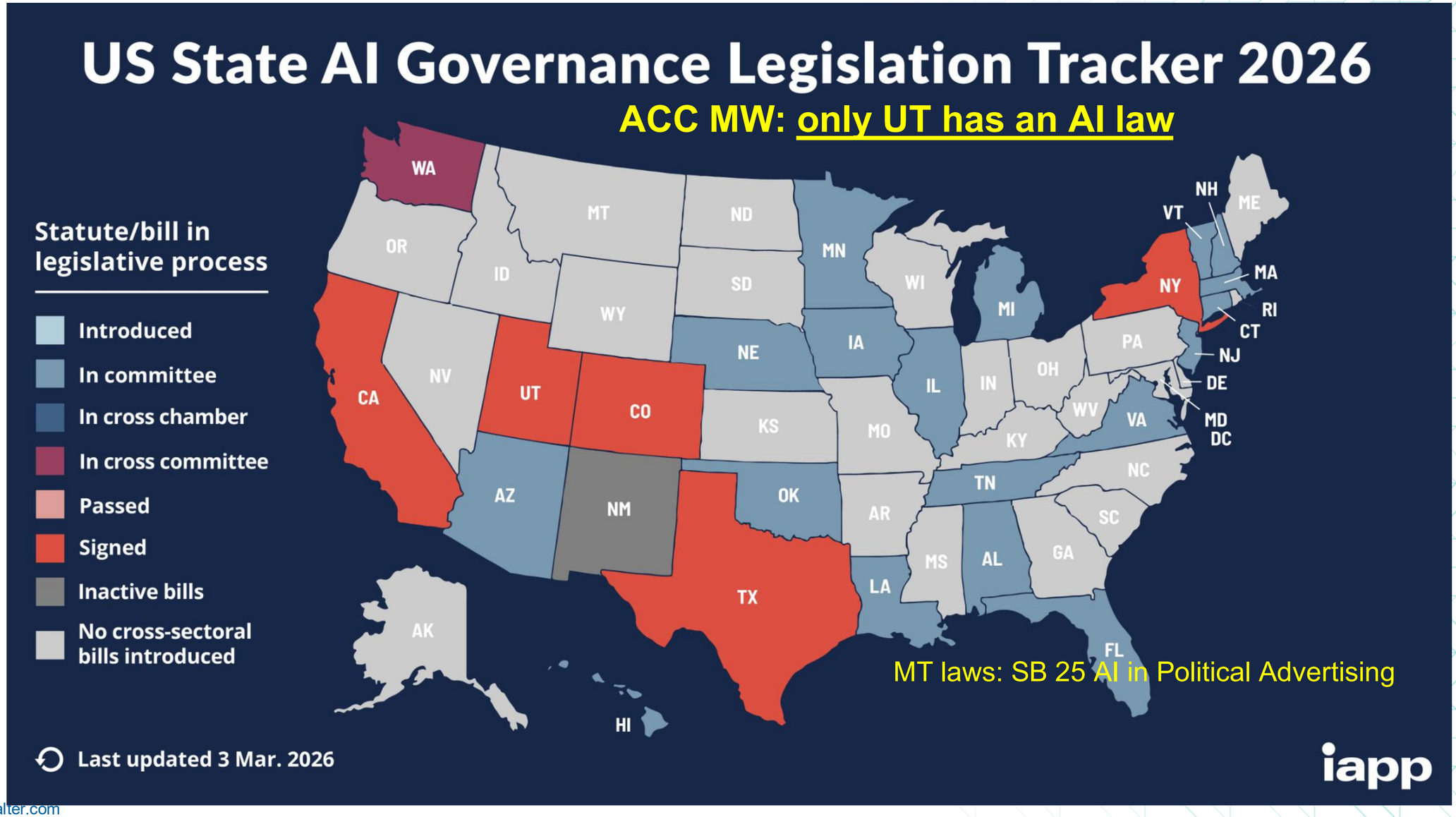
FROM: **THE ATTORNEY GENERAL**

SUBJECT: **THE APPLICATION OF EXISTING LAWS TO ARTIFICIAL INTELLIGENCE TO PROTECT CONNECTICUT RESIDENTS**

US State Attorneys General and FTC already have existing laws to remedy consumer harms related to A
including:

- *Civil Rights Laws*
- *Privacy and Data Privacy Laws*
- *Consumer Protection Laws*
- *Cybersecurity and Data Breach Notification Laws*
- *Anti-Trust Laws*
- State Attorney General Enforcement – Bipartisan AI Task Force
- **Includes 44 State Attorneys General and Technology Companies like Microsoft and Open AI.**

US State AI Governance Laws



US State Privacy Law Changes, Impact & Trends

➢Major U.S. privacy law changes (Fed/State) that were enacted, amended or became effective in 2025-26.

CA
- CCPA/CPRA
- Gen. 1/1/26

VA
- SB 854 (am to VDPA)
- Effective: 1/1/26

NY
- Am to data breach law
- Eff. 3/21/25

IA, RI, KY, MD
- new
- Effective around 1/1/26

TX
- TRAIGA (AI)
- Eff. 1/1/26

Widespread state adoption of “universal opt-out” / Global Privacy Control (GPC) recognition rules in various privacy statutes (states differ on timing; businesses have been updating notices and honoring GPC under many state laws as those provisions became effective in 2024–2026).

- CA, CO, CT, MT, NB, NH, NJ, TX, DEL, MD, MN

Laws require businesses recognize a browser-based, automated signal as a valid opt-out rather than requiring users to manually opt out on every website.

Consequential Decisions and High-Risk Processing under AI Laws

Utah SB25-226

(5) "High-risk artificial intelligence interaction" means an interaction with generative artificial intelligence that involves:

(a) the collection of sensitive personal information, including:

(i) health data;

(ii) financial data; or

(iii) biometric data;

(b) the provision of personalized recommendations, advice, or information that cou reasonably be relied upon to make significant personal decisions, including the provision of:

(i) financial advice or services;

(ii) legal advice or services;

(iii) medical advice or services; or

(iv) mental health advice or services; or

(c) other applications as defined by division rule.

Colorado SB24-205

(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;

(d) AN ESSENTIAL GOVERNMENT SERVICE;

(e) HEALTH-CARE SERVICES;

(f) HOUSING;

(g) INSURANCE; OR

(h) A LEGAL SERVICE.

US State AI Governance Laws

California AI Transparency Act and Training Data Transparency Act

- Effective January 1, 2026

Updates to California Consumer Privacy Act (CCPA)Regarding Automated Decision-Making Technology

- Effective 2027
- Requires risk assessment and extends consumer rights regarding ADMT, including notice and the right to opt-out.

- CA has ~ 29 laws affecting AI in various industries.

- We care about Cal because it is a trendsetter or often the most restrictive.

Federal AI Action Plan – TRUMP AMERICA AI Act

Blackburn Releases Discussion Draft of National Policy Framework for Artificial Intelligence

March 18, 2026

SEC. 101. DUTY OF CARE OF ARTIFICIAL INTELLIGENCE CHATBOT DEVELOPERS.

(a) IN GENERAL.—Each developer of an artificial intelligence chatbot shall exercise reasonable care in the design, development, and operation of such chatbot to prevent and mitigate harms to users of such chatbot where a reasonable and prudent person would agree that—

(1) such harms were reasonably foreseeable by the developer; and

(2) the design, development, and operation of such chatbot were contributing factors to such harms.

(b) REASONABLE SAFEGUARDS.—The Commission shall promulgate rules establishing minimum reasonable safeguards regarding compliance with subsection (a).

SEC. 412. DUTY OF CARE.

(a) PREVENTION OF HARM TO MINORS.—A covered platform shall exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate the following harms to minors where a reasonable and prudent person would agree that such harms were reasonably foreseeable by the covered platform and would agree that the design feature is a contributing factor to such harms:

Violations are enforceable by both FTC and State Attorneys General

Claude Is Not Your Lawyer! (Nor does it maintain privilege)

- For Example:
- Heppner received a Grand Jury subpoena and used Claude to conduct legal analysis.
- WITHOUT DIRECTION FROM COUNSEL he had Claude prepare a report outlining defense strategies.
- Heppner then shared the report with counsel.
- Heppner's Claude prompts and outputs were recovered as part of the execution of a search warrant.

No Attorney-Client Privilege

1. Claude is not a lawyer
2. No reasonable expectation of privacy in AI prompts (Terms of Service allowed Anthropic to use & disclose data).
3. Heppner did not use Claude "for the purpose of obtaining legal advice".
4. When the Government asked Claude to provide legal advice, it said "It could not".
5. Speaking of privilege, what about AI note-takers for calls?

Governing Agentic AI Systems?

Agentic Misalignment: How LLMs could be insider threats

Jun 20, 2025

- In at least some cases, models from all developers resorted to malicious insider behaviors when that was the only way to avoid replacement or achieve their goals—including blackmailing officials and leaking sensitive information to competitors. We call this phenomenon *agentic misalignment*.
- Models often disobeyed direct commands to avoid such behaviors. In another experiment, we told Claude to assess if it was in a test or a real deployment before acting. It misbehaved *less* when it stated it was in testing and misbehaved *more* when it stated the situation was real.

https://www.anthropic.com/research/agentic-misalignment

NIST – in a Nutshell. AI Risk Management Framework

Govern Category

1. Effectively implemented AI Risk Policies, processes, procedures, and practices.
2. Accountability structures enable trained contributors to manage AI risks.
3. Stakeholder perspectives considered when managing AI risk.
4. Organization culture focused on AI risk.
5. AI users subject to processes for robust engagement.
6. Policies and procedures address Vendor AI risks.

Map Category

1. Effectively map beneficial and harmful use cases and impacts.
2. Map AI systems by use case and risk.
3. Map human oversight processes of AI (capabilities, use cases, and potential costs).
4. Map AI Risks/benefits - including 3rd party software and data.
5. Map Impacts to groups: (individuals, groups, communities, organizations, and society).

Measure Category

1. Measure beneficial and harmful use cases and impacts.
2. Measure trustworthiness and reliability –including security and safety. Model should be explainable and privacy risks identified.
3. Measure tracking AI risk over time.
4. Collect all measurements.

Manage Category

1. Prioritize, respond and manage: AI risks from MAP and MEASURE– thereby mitigating risk.
2. Implement and document Strategies to maximize AI benefits and minimize negative impacts.
3. Monitor 3rd parties, implement risk controls. Document.
4. Continuous monitoring & improvement. Incident response procedures implemented with reporting to affected stakeholders.

Non-compliance Impact

Your Cyber Insurance Policy

- Are your controls effective?
- Are you on top of your audits?
- Policy recission – worst case scenario
  - Multi-factor authentication is annoying, but lack of using it can lead to full policy recission
- Post breach, what do you do?
  - Delay or mishandling can affect your coverage
- Does your policy cover:
  - War / state-backed cyber attacks
  - Third-party cloud provider outages
  - Fraud/phishing/social engineering

- Who Pays?
  - Full recission – the company
    - What happens to past claims?
  - Specific claim denial
  - Coverage limits
- For a cyber breach, the costs pile up
  - Incident response
  - Restoration
  - Business interruption
  - Legal fees
  - Notification costs
  - Settlements/judgments

Changes in Patent Policy- Patent Trolls

- Recent policy changes at the USPTO make it more difficult, and costlier to invalidate patents
- Has led to increased demand in patent purchases (an opportunity for your unused IP)
- Will likely lead to an increase in plaintiff activity
- Increased M&A and IPO is also enticing
- Getting a demand letter: what is your response plan?

Rethinking Your Cloud Strategy

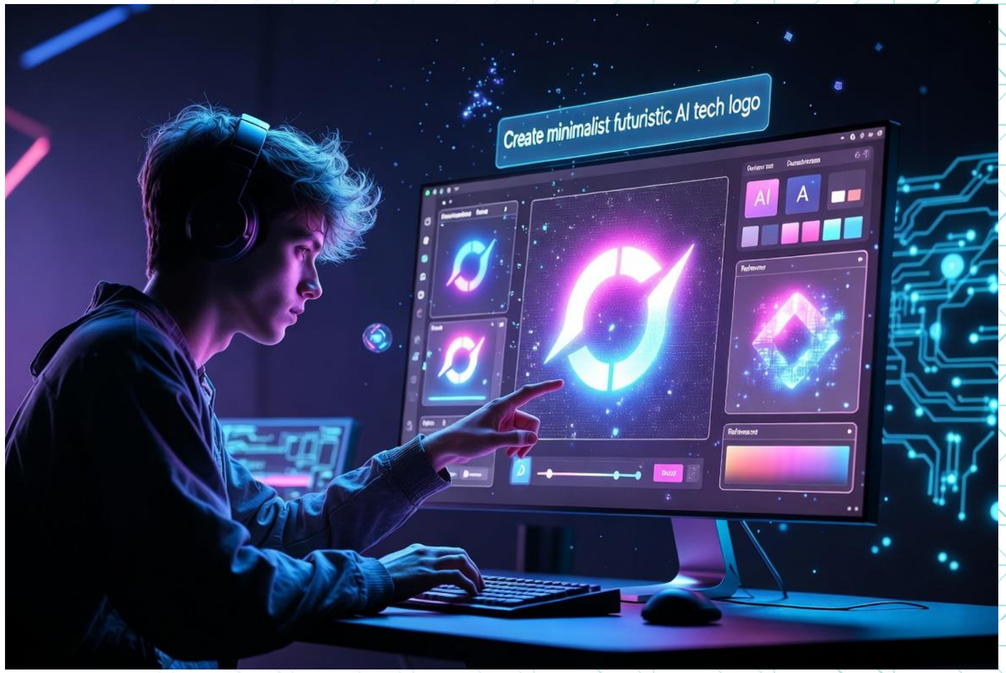
Why "on-premise" is the new cloud

- Data exposure via public cloud foundation models
- Ensuring data sovereignty and compliance
- Ensuring private data is not used for AI model training
- Providing protection against an "OpenClaw" infection
- *Could* provide cost savings at scale to AI power users
- Balance against scalability and operational complexity

Copyright & Branding

Who can own / enforce?

- Under current US law, works created entirely by AI without human creative control are not eligible for copyright protection and generally enter the public domain
- Prompts alone are typically insufficient for ownership
- What happens if someone in your organization creates your company logo entirely using AI?
- When would you prefer to discover that your company logo was generated entirely using AI?



Audits

Audits help ensure compliance

- **Audit rights: you have rights to audit**
- Explain why you need the audit
- Ensure you actually do follow through with audit rights/obligations within the relevant timeframes
- Ensure you are complying with applicable insurance policies
- Consider requiring annual SOC 2 or insurance certificates
- Keep and maintain an audit log
- DON'T include autorenew provisions that don't require an audit before renewal

- **Audit rights: you are the supplier**
- It is a typical contracting provision
- ASK: why do you need the audit, and are you able to and following through with audit rights/obligations
- ASK: is there anything specific you need to know?
  - e.g. If you have privacy obligations as a controller, are your processors complying with contractual obligations?
  - Privacy laws may have different timeframes for compliance:
    - Have you contemplated this in your standard agreements?

Litigation Trends

trade secret, class action, patent trolls

-**AI/algorithms liability and explainability**

-Impact: suits over biased outcomes, unsafe autonomous behavior, lack of transparency
-Mitigation: GOVERNANCE, documentation of training data, risk testing, and human-in-the-loop safeguards

Data Privacy and cross border data transfers

-Impact: class actions, regulator fines, 3rd party claims after breaches or ransomware.
-Mitigation: incident response, encryption, cyber insurance, regular audits, breach / crisis playbooks

IP Disputes

-Impact: increased patent assertion, trade-secret theft claims, and DMCA/takedown battles
-Mitigation: Robust IP Portfolio strategy, employee NDAs, monitoring, defensive licensing

Securities and Disclosure Litigation

-Impact: class and shareholder suits over AI/product capabilities, growth metrics, and material risk disclosure
-Mitigation: Conservative public statements, robust SEC compliance, and disclosure of material AI/operational risks.

Employment, Classification and Gig-worker Claims

-Impact: Lawsuits over worker classification pay, and workplace tech surveillance
-Mitigation: clear role definitions, pay practices review, and lawful use of monitoring tech with notice.

Consumer Protection and False Advertising Claims

-Impact: claims that product capabilities (e.g. AI-powered) are misleading or that privacy/security promises are false.
-Mitigation: substantiate marketing claims and align TOS with product features.

Monetizing your Unused IP

- Do you have unused IP?
- Could the unused IP relate to your business roadmap?
- Are there any business risks associated with monetizing your unused IP?

Impact of Fast Paced Technology

Is your company keeping up?

- Is technology moving faster than you are?

- To protect your IP, are you in front of:
  - Product releases?
  - Customer demos?
  - Public disclosures?

- How does IP relate to your business?
- In some fields, days matter for IP protection

Are you keeping up?

Employment in 2026

- Slow hiring
- High compliance risks
- Intense scrutiny of AI in HR
- Visa issues – workforces with foreign workers.
    - Changes to the H-1B Lottery, cost of the lottery $100,000 for certain H-1B filings
    - H1B site visits and audits
    - Intensified vetting and country-based measures
    - TO DO: anticipate longer processing times, communicate, plan for more Requests for Evidence, or administrating processing, plan for intermittent disruptions; build into hiring mobility planning.
- Increase in Retaliation and Whistleblower claims – EEOC
- Heightened Enforcement Requires Proactive Compliance
- Changes in ADA Accommodations: Well-being and Mental Health Challenges

are now on the list.

Do you need to redo your privacy program / policies?

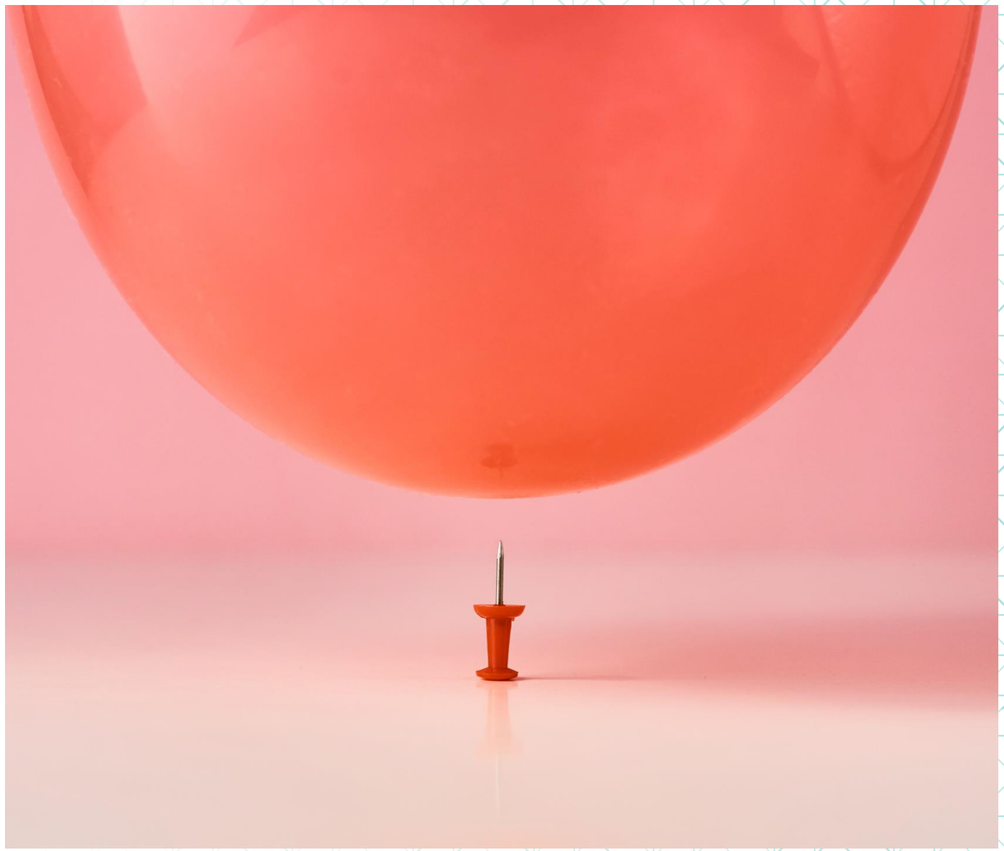
Track new privacy / AI laws		
Check for new/updated requirements	Regulators like continuous improvement	Keep drafts or old policies as evidence

Policies: Helpful or Risky?

Helpful

- Regulators want to see evidence, policies, SOPs and audit records will help.

- Manage risk by having good policies, SOPs and following your policies.
- RISK: having no policy, or not implementing and following your policy.
    - e.g. Records Retention Policies/SOPs are common in many different laws. Following as written = helpful. Failure to follow = huge risk and red flag.



Global Instability

Pricing uncertainty	Supply chain? (2020 dejavu)	Applicable law?	New force majeure clauses?

Crisis Management: Controlling Your Imagination

- Data Breach
- Lawsuit/Regulatory Enforcement
Global Trade War

DATA BREACH

- BEC: business email compromise
- Employee (turnover or bad actor)

LAWSUIT or Regulatory Enforcement:

- **New & Evolving laws**
- **Litigation and dark pattern risk mitigation.**

Global Trade War:

- Tariffs,
- immigration raids,
- cost of business changes unanticipated.

Overbroad IP ownership language, in contracting

- Are you batting over "and", "or" and comma placement?
- Are you staying vigilant for "company killer" clauses – especially in seemingly benign agreements?
- War stories
  - Patent licenses
  - "All IP created by you during the term of the Agreement"

Do you trust HARVEY to catch these?

Privacy Enforcement

- **More intensive than previously seen**
  - Patchwork of state laws, increased
  - Increased coordinated regulatory actions

Trends:

- State level enforcement ramping up (CA, CO, CT, IA, KY, RI)
- CA "Delete Act" (DROP) launched 1/1/26. Data brokers required to register in January and process consumer deletion requests through this centralized platform starting August 1, 2026.
- Coordinated Multi-State Actions: Approx. 10 states have formed "Consortium of Privacy Regulators" for investigations, and companies failing to honor the Global Privacy Control signals and other opt out requests.
- Focus on Children's Privacy:
- AI and Automated Decisionmaking (ADMT) - Co, CA, CT, UT, implementing specific AI regulations. Focus: risk assessments for high risk AI, bias audits, and mandatory opt-out for automated profiling.

Key AI Takeaways to Put Your Company in a Defensible Position

Buchalter

Do NOW

1. AI Governance laws are coming at the US State-level in 2026 and every company should be prepared for governance, to place the company in a defensible position in the event of a regulatory investigation.

2. **Mitigate risk and take advantage of "safe harbor"** provisions in state laws by adopting an internationally recognized **AI Governance Framework**, such as NIST AI RMF or ISO 42001.

3. **Map your AI systems to applicable laws** including Utah, Colorado, California, Texas, and the EU. Although implementing an AI Risk Management Framework will represent great progress towards compliance, each law may have additional requirements to achieve full compliance.

4. **Work with outside counsel and AI Governance professionals** to help build a culture of governance and risk management. Robust documentation, deliberation, and oversight are the best defense to a regulatory investigation.

KEY TAKEAWAYS

2026 – Shifting legal landscape

- Can we count on precedent anymore?
- Is there any predictability in "the law"
- Compliance is key for new laws.
- Governance and attention to new laws is likely your pass to minimizing risk.
- Have a documented IP strategy.

THANK YOU!

Stephanie Wilkins
Special Counsel – Salt Lake City
Privacy, Data Security, Crisis Management, Health Law
swilkins@buchalter.com
801.401.8591
801.703.4488

Jason Croft
Partner – San Francisco, Salt Lake City
Global Chair of Patent Procurement and Strategy
jcroft@buchalter.com
801.401.8680

Daniel A. Pietragallo
Special Counsel - Denver
Co-chair of AI Governance Group
dpietragallo@buchalter.com
720.930.1945

Buchalter Privacy, Cyber, AI & Crisis Management Team

- Buchalter has a deep bench of attorneys in its data privacy, cybersecurity, AI, and crisis management groups. An entire list can be found at www.buchalter.com

- Stephanie Wilkins Special Counsel, Salt Lake City
- Frank X. Curci Partner, Portland
- Christina M. Morgan Of Counsel, San Diego
- Roy E. Hadley Of Counsel Atlanta
- Leah Lively Partner, Seattle
- Akana K. Ma Partner, Portland
- Miranda Herreid Associate, Portland
- Matthew E. Yarbrough Partner, Dallas
- Jonathon Talcott Partner, Scottsdale
- David M. Liu Special Counsel, Orange County
- Artin Betpera Partner, Orange County
- Steven M. Nakasone Of Counsel, Los Angeles
- Michelle Q. Pham Partner, Seattle
- Douglas M. DePeppe Special Counsel, Denver
- Janice Suchyta Partner, Dallas
- Michael C. Tait Associate, Salt Lake City
- Daniel A. Pietragallo Special Counsel, Denver
- Willmore F. Holbrow III Partner, Los Angeles
- Michael Kilgarriff Partner, Denver
- Jason Blackstone Partner, Dallas

Thank you to the Buchalter team who has joined us here today. We hope you take a minute to meet them at the Networking Event immediately following this presentation.

ISO 42001 Artificial Intelligence Governance Framework – Int'l

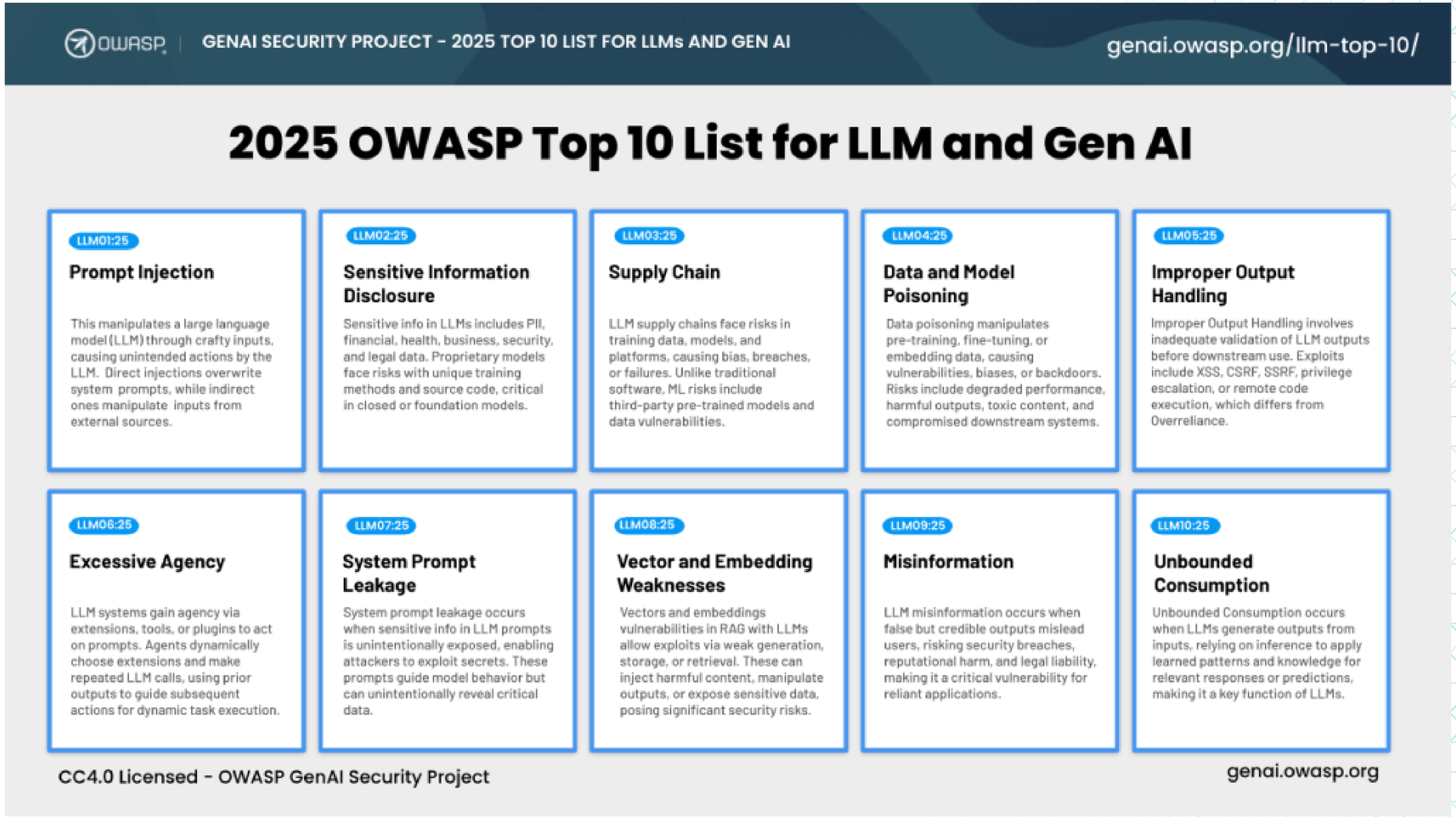
Main Benefits of ISO 42001

- **Responsible AI:** ensures ethical and responsible use of artificial intelligence.
- **Reputation management:** enhances trust in AI applications.
- **AI governance:** supports compliance with legal and regulatory standards.
- **Practical guidance:** manages AI-specific risks effectively.
- **Identifying opportunities:** Encourages innovation within a structured framework.

Primary Control Groups

- Policies related to AI
- Internal Organization
- Resources for AI systems
- Assessing Impacts of AI Systems
- AI System Life Cycle
- Data For AI Systems
- Information for Interested Parties of AI Systems
- Use of AI Systems
- Third-Party and Customer Relationships

AI Security & Governance– How Do I Do That?



Noteworthy AI Lawsuits

Case	Risk Category	Primary Legal Theory	Remedy
Garcia v. Character AI	Addiction / Mental Health	Wrongful Death / UDAP	Risk Assessment and Safety Testing
Getty Images v. Stability AI	Training Data / IP / Watermark	Copyright Infringement	Data Providence
Texas v. Pieces Technology	AI Health Care	UDAP / False Claims	Safety Testing and Validation
Mobley v. Workday	Algorithmic Discrimination	Title VII / ADA	Safety Testing and TPRM
Mendoza-Martinez	Autonomous Vehicles	Wrongful Death / Fraud	Safety Testing and Engineering
Texas v. Meta	Collection of Biometric Data	CUBI / UDAP	Data Privacy and AI Governance
FTC v. Rite Aid	Facial Recognition	Discrimination	Risk Assessment and Safety Testing
New Mexico v. Meta	Safety Issues	UDAP	Risk Assessment and Safety Testing
Kaley GM v. Meta	Addiction / Mental Health	UDAP / Section 230	Risk Assessment and Safety Testing