Chamberlain Hrdlicka

ACC Association of Corporate Counsel HOUSTON

PRIVACY & DATA SECURITY IN 2025: A COMPREHENSIVE LEGAL LANDSCAPE FOR CORPORATE COUNSEL

Aly Dossa, Shareholder, Chamberlain Hrdlicka
Mohammad Totonchian, Deputy General Counsel, Altus Group
Marcus Burnside, Senior Associate, Chamberlain Hrdlicka

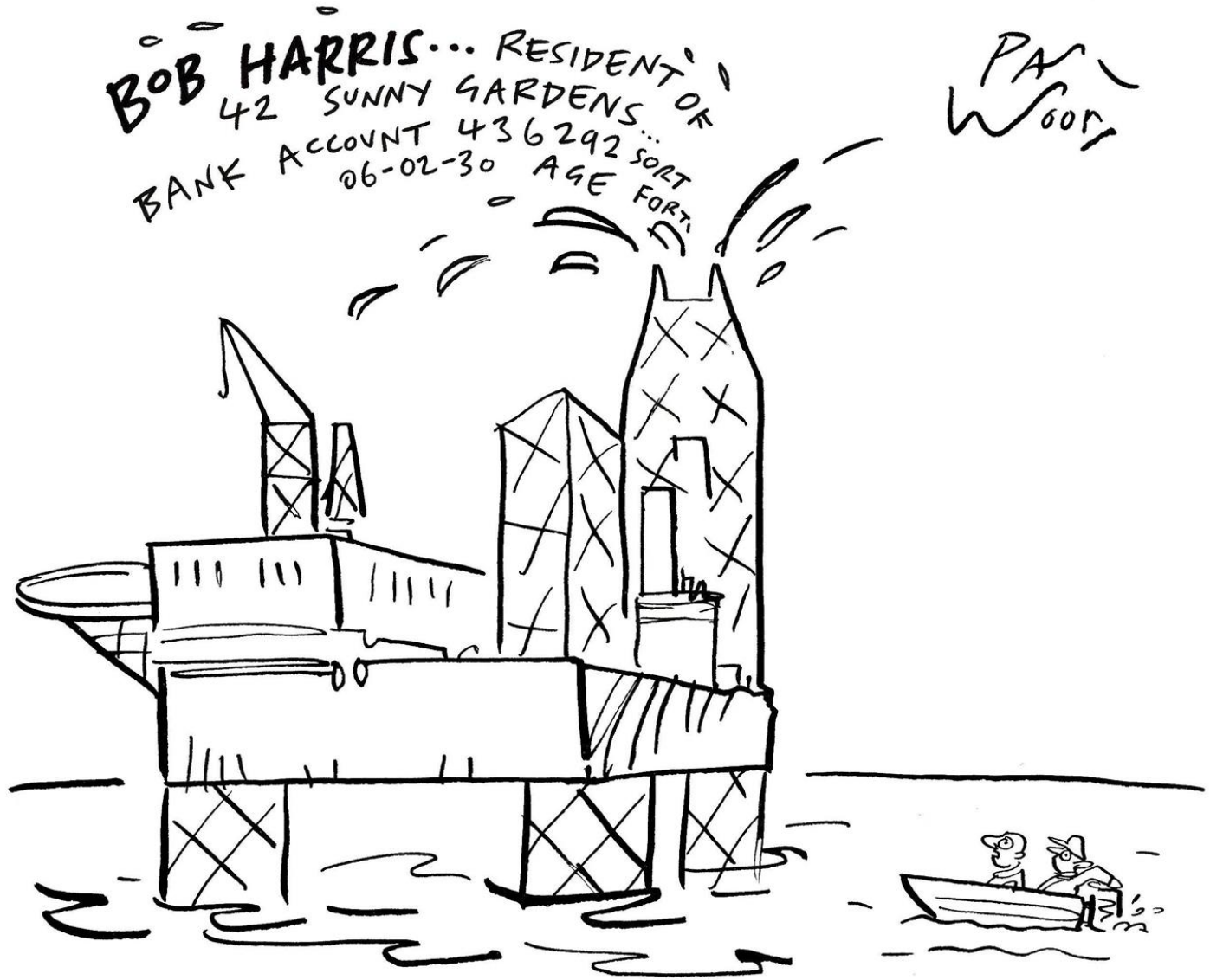
PRESENTATION OUTLINE

1. State Privacy Law Update
2. Cyber Security Trends and Best Practices
3. Practical Guide to Implementing AI in Your Organization

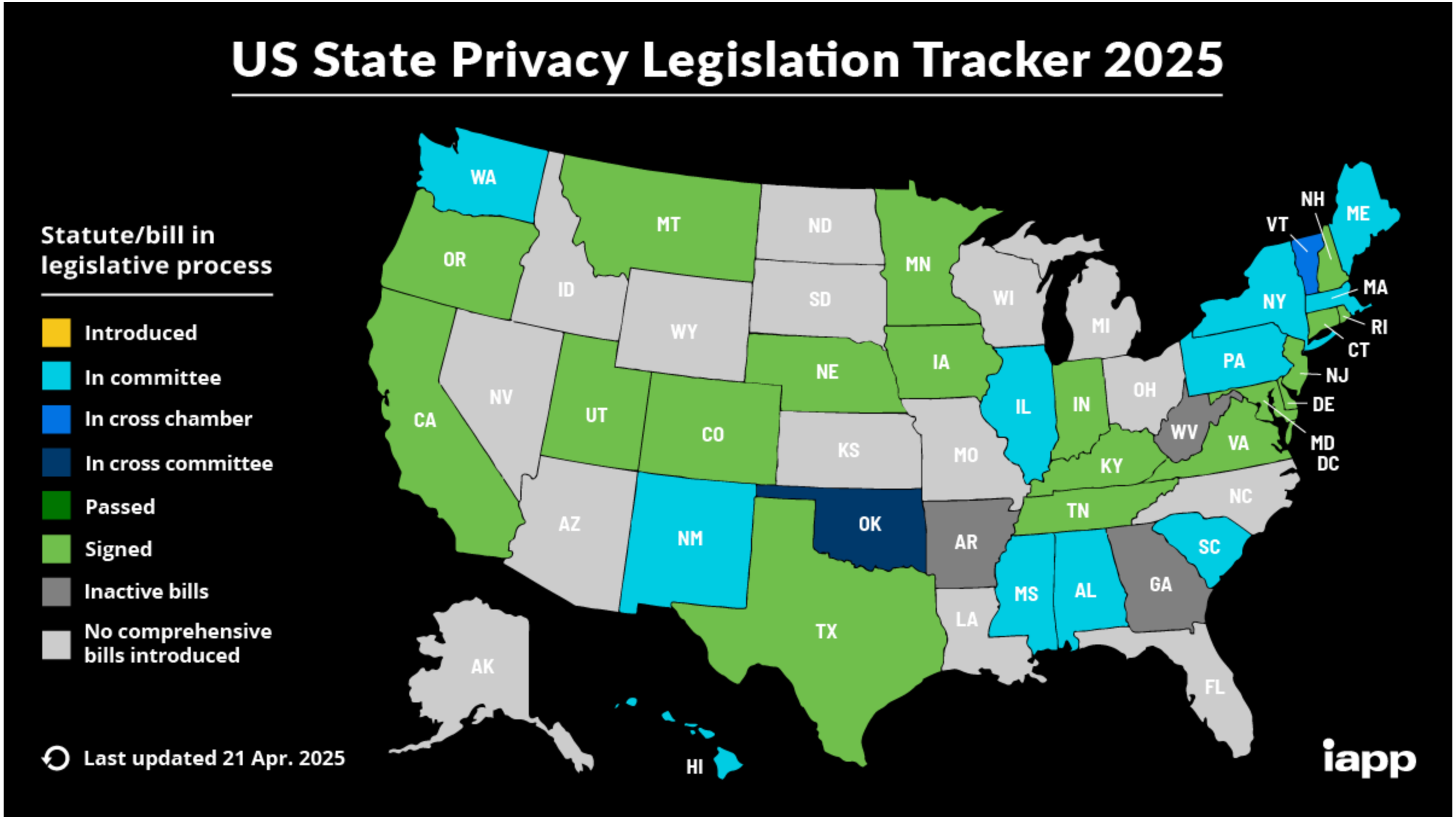
Chamberlain Hrdlicka

State Privacy Law Update

ACC Association of Corporate Counsel HOUSTON



US State Privacy Legislation Tracker 2025



PRIVACY LAWS COMING ONLINE SOON (2025)

1. **Colorado Biometric Privacy Law** – July 1, 2025
   - Covers employee biometric data
2. **Tennessee Information Protection Act** – July 1, 2025
3. **Oregon Consumer Privacy Act** – for non-profits, July 1, 2025
4. **New Jersey Universal Opt-Out Mechanism** – July 15, 2025
5. **Minnesota Consumer Data Privacy** – July 31, 2025
   - First state of require data inventories
6. **Maryland Online Data Privacy Act** – October 1, 2025
   - Shifting to requiring data minimization and departing from notice-and-consent paradigm

PRIVACY LAWS COMING ONLINE SOON (2026)

1. **Indiana Consumer Data Protection Act** – January 1, 2026
2. **Kentucky Consumer Data Protection Act** – January 1, 2026
3. **Rhode Island Consumer Privacy Act** – January 1, 2026
4. **Delaware Universal Opt-Out Mechanism** – January 1, 2026
5. **Oregon Universal Opt-Out Mechanism** – January 1, 2026

PRIVACY ENFORCEMENT REGULATORY TRENDS

1. Texas has become a leader in privacy enforcement.
2. Improper data collection issues are being addressed using a combination of privacy laws and consumer protection laws.
   - E.g., Deceptive trade practice laws
3. Fast tracking (at least in Texas) of data privacy cases by the Texas attorney general in state court.
4. Consent/settlement agreement result:
   - Deletion of tainted data sets
   - Deletion of AI models generated from tainted data sets
   - Preventing sale of data to third parties for a period of time
5. Creation of the Consortium of Privacy Regulators (CA, CO, CT, DE, IN, NJ, OR)

INSIGHT FROM STATE PRIVACY REGULATORS FROM IAPP GLOBAL PRIVACY SUMMIT

1. State attorney generals are sharing information and resources on privacy enforcement.
2. State attorney generals want you to "show your work" related to implementing your privacy programs.
3. They appear to disfavor general privacy notices – they want to see that the privacy policy is directed to their state's laws.
4. If you believe that there is an ambiguity in the law, they want you to interpret the law in the most pro-consumer manner.
5. States that are enacting or amending their privacy laws are looking to see "what worked" and "what did work" in other states
6. U.S. Regulatory approach vs EU Regulatory approach

Chamberlain Hrdlicka

Cyber Security Trends & Best Practices

ACC Association of Corporate Counsel HOUSTON

CYBER SECURITY TRENDS & BEST PRACTICES – NORMAL OPERATIONS

1. Like privacy issues, have written plans and procedures and justifications for decisions made for each.
2. Shield you CISO. Your CISO needs to be candid with leadership, but this can create external risk. Mitigate this risk by:
   - Using outside counsel to maintain privilege for strategic meetings and for assessments
   - Strictly limiting public statements made by CISO
3. Find commonalities between cyber protection and privacy/data governance to leverage IT resources instead of legal resources.

THREAT ACTOR TRENDS

1. AI is making attack vectors more effective.
2. Focusing more on exfiltration of data instead of ransomware.
3. Dwell time is decreasing.
4. Average demand amounts are leveling out.
5. Pressure tactics are becoming more personal to organization's decision makers.

POST-BREACH BEST PRACTICES

1. Engaging breach resources through outside counsel to maintain privilege.
2. Engage FBI to pursue potential notification waiver – national security waiver is most likely option.
3. Informal notices to state regulators prior to official notices is the regulator's preference.
4. **FOLLOW YOUR PLAYBOOK!**

Chamberlain Hrdlicka

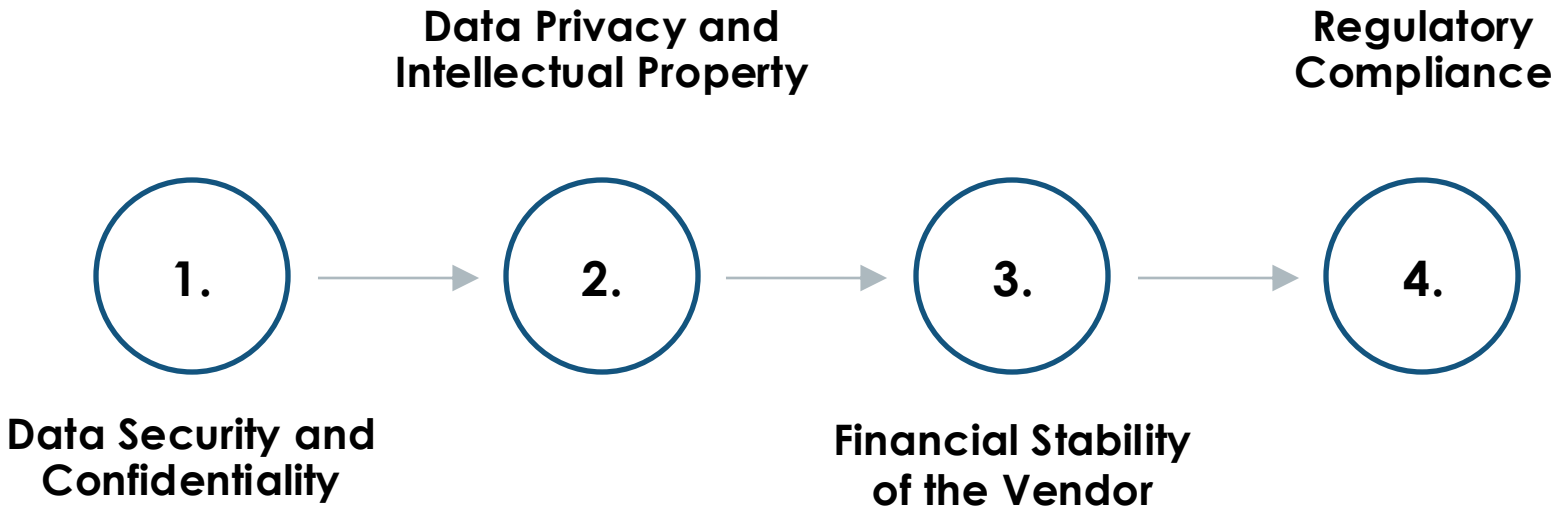
Practical Guide to Implementing AI in Your Organization

ACC Association of Corporate Counsel HOUSTON

AI REGULATORY STATUS

1. **Utah AI Policy Act** – Effective May 1, 2024
2. **California Assembly Bill 2013 – Artificial Intelligence Training Data Transparency** – Effective January 1, 2026
3. **California Senate Bill 942 – California AI Transparency Act** – Effective January 1, 2026
4. **Colorado AI Act** – Effective February 1, 2026
5. **FTC still very interested in AI**

KEY FACTORS IN AI TOOL PROCUREMENT



DATA SECURITY AND CONFIDENTIALITY

1. Data use limits ensure no sensitive data is reused or shared without contractual consent.
2. Confidentiality and breach terms.
3. Security and compliance.

FINANCIAL STABILITY OF THE VENDOR

1. **Long-term Viability**
   - Assess financial health to reduce risk of service disruption.
2. **Continuity Planning**
   - Require contingency plans for bankruptcy or acquisition.
3. **Exit Terms**
   - Consider what happens at the end of the term.

REGULATORY COMPLIANCE

1. **Jurisdictional Fit**
   - Ensure the tool complies with applicable laws
     - E.g., GDPR, HIPAA
2. **Auditability**
   - Confirm the vendor can support audits or regulatory inquiries.
3. **Ongoing Monitoring**
   - Require updates to keep pace with evolving legal standards.

KEY TAKEAWAYS ON IMPLEMENTING AI TOOLS

1. Important to engage stakeholders from Legal, IT, Compliance, Privacy, Security, Risk, Audit, Marketing, and HR.
   - This is not an "IT" only issue.
2. Vendors are including AI-specific terms via AI Addendums to standard SaaS agreements.
3. Successfully implementing an AI tool requires that it be accompanied by a training program and that it is consistent with company's AI policy.

Chamberlain Hrdlicka

Questions?

ACC Association of Corporate Counsel HOUSTON

Chamberlain Hrdlicka

THANK YOU

ACC Association of Corporate Counsel HOUSTON