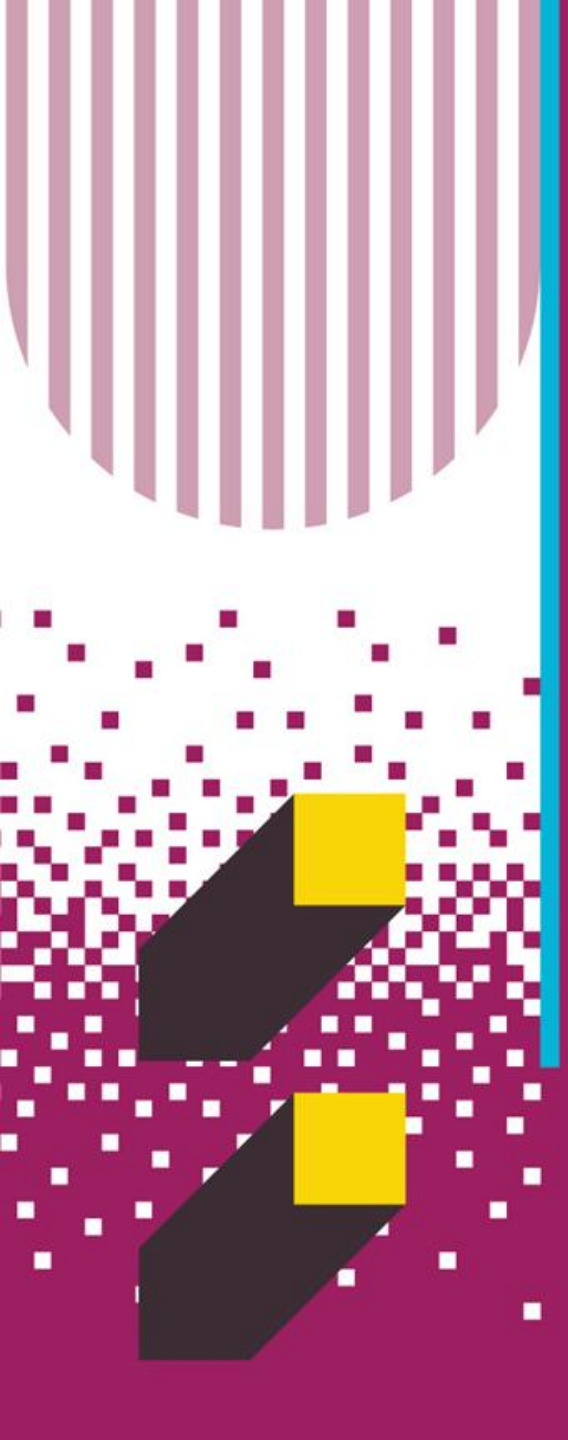


IAPP Canada Symposium 2026

Privacy | AI governance | Cybersecurity law

Conference 4-5 May
Workshops 6 May
Training 6-7 May
TORONTO

#IAPPSymposium26

WHAT IN THE WORLD?

The Privacy and AI Landscape South of the Border

WELCOME AND INTRODUCTIONS

Stacey Gray

Senior Director for U.S. Policy

Future of Privacy Forum

Brandon Kerstens

Vice President, Associate General Counsel, Chief Privacy Officer

Match Group

Gabe Maldoff

Partner

Goodwin Procter

Karen McGee

Former Chief Privacy Officer

Levi Strauss

AGENDA OUTLINE

I. Welcome and Introductions
II. Patchwork Nation: The Fragmented US Digital Regulation
III. Key Themes In Regulation, Enforcement and Litigation
    i. Digital Advertising and Its Discontents
    ii. Sensitive Data, National Security and Reputation
    iii. Online Safety
    iv. The Emerging Law(s) of AI
IV. Questions

Patchwork Nation: The Fragmented US Digital Regulation

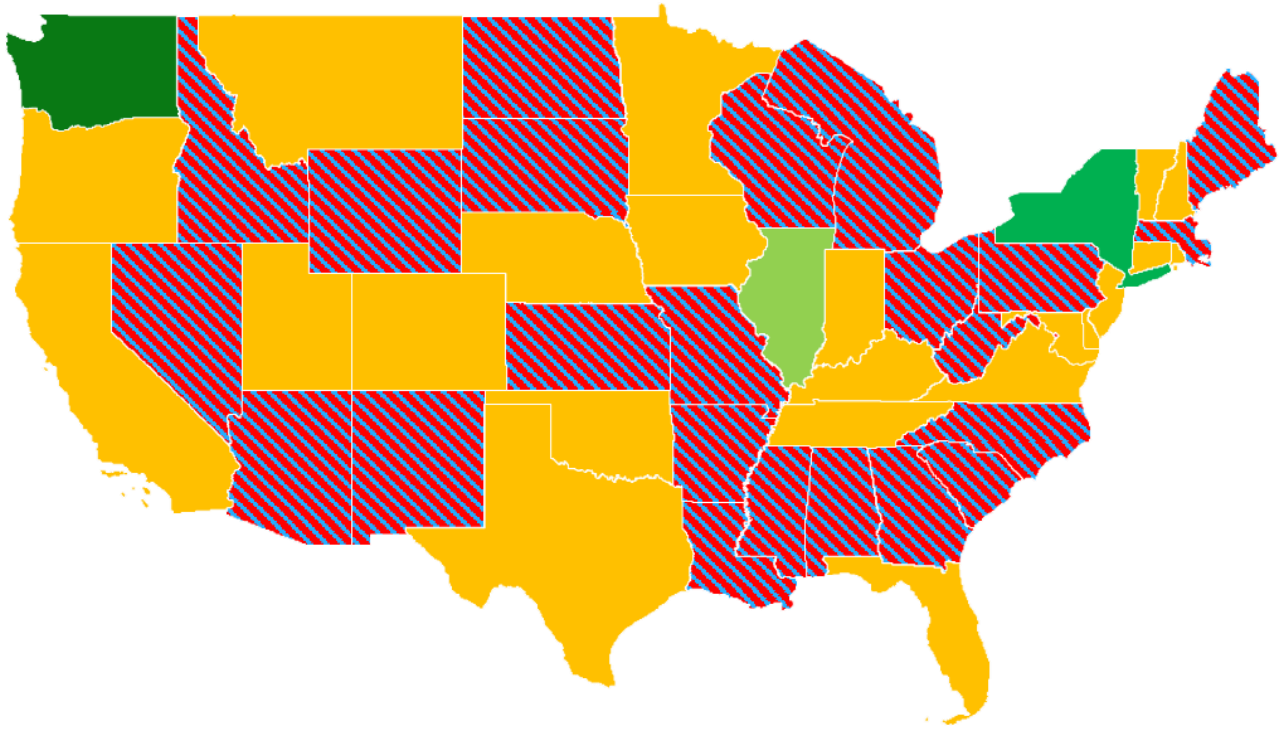
Consumer Protection Statutes
- E.g. FTC Act Section 5
- Prohibit “unfair or deceptive” conduct

Anti-Spam Laws
- E.g. CAN-SPAM, TCPA
- Regulate unsolicited communications

Sectoral Privacy Laws
- E.g. HIPAA, GLBA, FERPA
- Regulate specific sectors

State Consumer Privacy Laws
- E.g., CA, VA, CO, CT
- Comprehensive data protection rights

Issue- and Sector-Specific State Laws
- E.g., IL BIPA, NY CDPA, WA MHMDA



Moving Past the Headlines: The Wild West?

- **Shift from sectoral protection to sectoral exclusion:** 21 states have enacted comprehensive privacy laws modeled to varying degrees on GDPR, with important exclusions for regulated sectors and small businesses.
- **Federalism as a force multiplier:** States play off each other, leading to compounding risk.
- **Politics drives enforcement priorities:** Privacy and digital regulation cross political lines, often driven by headlines.
- **Litigation creates zones of heightened risks:** Private rights of action drive legal risk.

Digital Advertising and its Discontents

- **Opt-out of Sale/Sharing & Universal Opt-Out Mechanisms (UOOMs / GPC):** Coordinated enforcement sweep (Sept 2025) (CA,CO,CT)
- **Recent enforcement signals:** Healthline ($1.55M) (July 2025) (health data + purpose limitation + deficient vendor contracts); Honda ($632k) (March 2025) (improper DSAR forms; asymmetric cookie banners), Tractor Supply ($1.35M) (Sept 2025) (ineffective opt-outs; deficient contracts),
- **Data Minimization & Risk Assessments** — Maryland's "reasonably necessary and proportionate" standard (strictest in U.S.); CCPA risk assessments now required for selling/sharing PI for targeted ads (Jan 1, 2026)
- **California DELETE Act** — universal deletion; consumer requests live Jan 2026, broker compliance Aug 1, 2026; $200/day/consumer for missed deletions; CalPrivacy launched a dedicated Data Broker Strike Force
- **Litigation Trends** — Wiretap Acts/CIPA – cookie banners, session replay, now AI...

Sensitive Data, National Security, and Reputation

- **Kids data as sensitive data:** Parental consent requirements for kids under 13; opt-in consent (or outright bans) for targeted advertising to teens; new flowdown requirements and intersection across state age verification laws.
- **Biometric privacy risks find new expressions:** Biometric litigation meets a new suite of AI-based tools.
- **Health data and inferences:** Regulators and litigators show increasing sophistication and technological knowhow.
- **Location data under the microscope:** From sensitive data restrictions to outright bans in Virginia, Oregon and Maryland.
- **National security as privacy:** Access to data by actors associated with China, Russia and other countries of concern likely to impact Canadian companies.

Online Safety: Age Verification & Youth Safety

Takeaway: The US is moving from "child privacy" to mandatory age assurance – but through a messy state-led patchwork.

- **Federal momentum, but no law.**
- **Age checks spreading beyond adult sites:** States are moving age assurance upstream to app stores, operating systems and platform design defaults.
- **Adult-content laws got major boost:** Free Speech Coalition v Paxton upheld Texas's age-verification law, reinforcing wave of adult-site age-gating laws.
- **Enforcement is becoming operational:** Roblox settlements show regulators using child-safety cases to demand product changes, not just penalties.

Online Safety: Content Moderation & Platform Liability

Takeaway: The liability theory is shifting from "you failed to moderate content" (blocked by 230) to "you designed an unsafe product."

- **Section 230 still matters but design claims getting around it.**
- **Plaintiffs reframing platforms as products:** Infinite scroll, autoplay, notifications, recommendation systems, and chat are being challenged as design choices.
- **Recent verdicts raise the stakes:** CA and NM cases show juries are receptive to youth-safety theories framed around addictive design platform architecture.
- **Practical implication:** a governance obligation – document design decisions, test youth-risk mitigations, and align public claims with risk controls.

The Emerging Law(s) of AI

- Moving through a mix of executive actions, agency guidance and state laws
- Federal policy emphasizes civil rights, fairness, transparency and accountability but *voluntary* vs binding
- All 50 states (including D.C. and territories) have introduced AI-related bills covering algorithmic discrimination, transparent disclosure, AI-generated content, government use and worker protections
- Current administration less focused on trustworthy AI and more focused on innovation and competitiveness

U.S. Legislation vs The EU AI Act

Feature	U.S. (Federal & State Patchwork)	EU AI Act (Single, Comprehensive)
Regulatory Model	Sectoral approach + agency enforcement + state laws; heavy use of guidance and existing ancillary laws (privacy, consumer protection, civil rights)	Horizontal, standalone AI regulation applying broadly across sectors, little linkage with other regulation
Core concepts	Risk and harm are central but not yet organized into a single statutory risk taxonomy; NIST AI RMF is voluntary but influential	Formal risk tiers: unacceptable, high-risk, limited-risk, minimal-risk, with obligations tied to category
Areas of focus	Executive orders, agency guidance (FTC, CFPB, EEOC, HHS, etc.), NIST AI RMF, state AI/ADM laws, consumer protection, privacy and anti-discrimination	Direct obligations on “providers” and “deployers” of AI systems and GPAI models; conformity assessments, technical documentation, CE-like regime
Scope	Varies by state and sector; examples: algorithmic discrimination, transparency, impact assessments, procurement rules, deepfake labeling	Detailed obligations for high-risk systems (data governance, documentation, human oversight, robustness, post-market monitoring) and transparency for chatbots/deepfakes
Enforcement	Mix of federal agencies + state AGs; penalties via existing statutes and new state AI laws (e.g., Colorado SB 24-205)	Significant administrative fines (up to the greater of €35M or 7% global turnover for certain

AI: Practically Speaking

AI Inventory & Classification

- Inventory of all AI systems (internal + vendor)
- Categorize by risk: consequential decisions, customer-facing, internal

Impact Assessments & Risk Management

- Impact Assessments for higher-risk uses
- Evaluate discrimination risk, privacy impacts, ADM
- Align to a framework (NIST AI RMF)

Data Governance & Controls

- Document decisions, mitigations, approvals.
- Maintain human review
- Cross functional working committee
- Policies for use, testing, approvals
- Test pre-deployment; monitor for drift, fairness, performance
- Deploy appropriate training
- Integrate AI risk into incident response plans

Transparency & Communication

- Provide notice when consumes interact with AI
- Label synthetic or AI generated content
- Offer plain language explanations

Consumer Rights

- Appeal mechanisms and human intervention paths
- Allow for correction of inaccurate data

Vendor Management

- Update contracts and monitor compliance
- Consider how AI affects needed security controls, permissible data use, etc.
- Update due diligence processes

Federal Landscape

- **(Still) No Federal Omnibus Privacy Law** – SECURE Data Act (House Energy & Commerce) is notably aligned with state laws; children's privacy; mid-terms approaching
- **FTC's Priorities:** Kids safety/COPPA; deception enforcement (Disney, Match/OkCupid, GM/OnStar); TAKE IT DOWN Act enforcement begins May 19, 2026

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Symposium 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!