What Cybersecurity Leaders Need to Consider for Privacy & AI Compliance

Cyber Symposium 2025

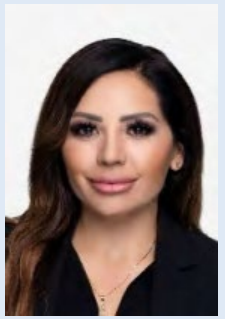
October 15, 2025

forvis mazars

Meet your presenters

Nikole Davenport, JD, LLM, CIPP-US, CIPM, FIP

Director



Diana Ramirez, MHA, CHC, CHPC

Manager

© 2025 Forvis Mazars, LLP. All rights reserved.

Agenda

1. Top 10 Concerns
2. New Privacy Legal Landscape
3. Enforcement Actions
4. AI Focus
5. Privacy Impact / Risk Assessments
6. Data Mapping
7. Third-Party Vendor Management
8. Privacy Trends
9. Change Management

© 2025 Forvis Mazars, LLP. All rights reserved.

Navigating Complexity

TRENDS

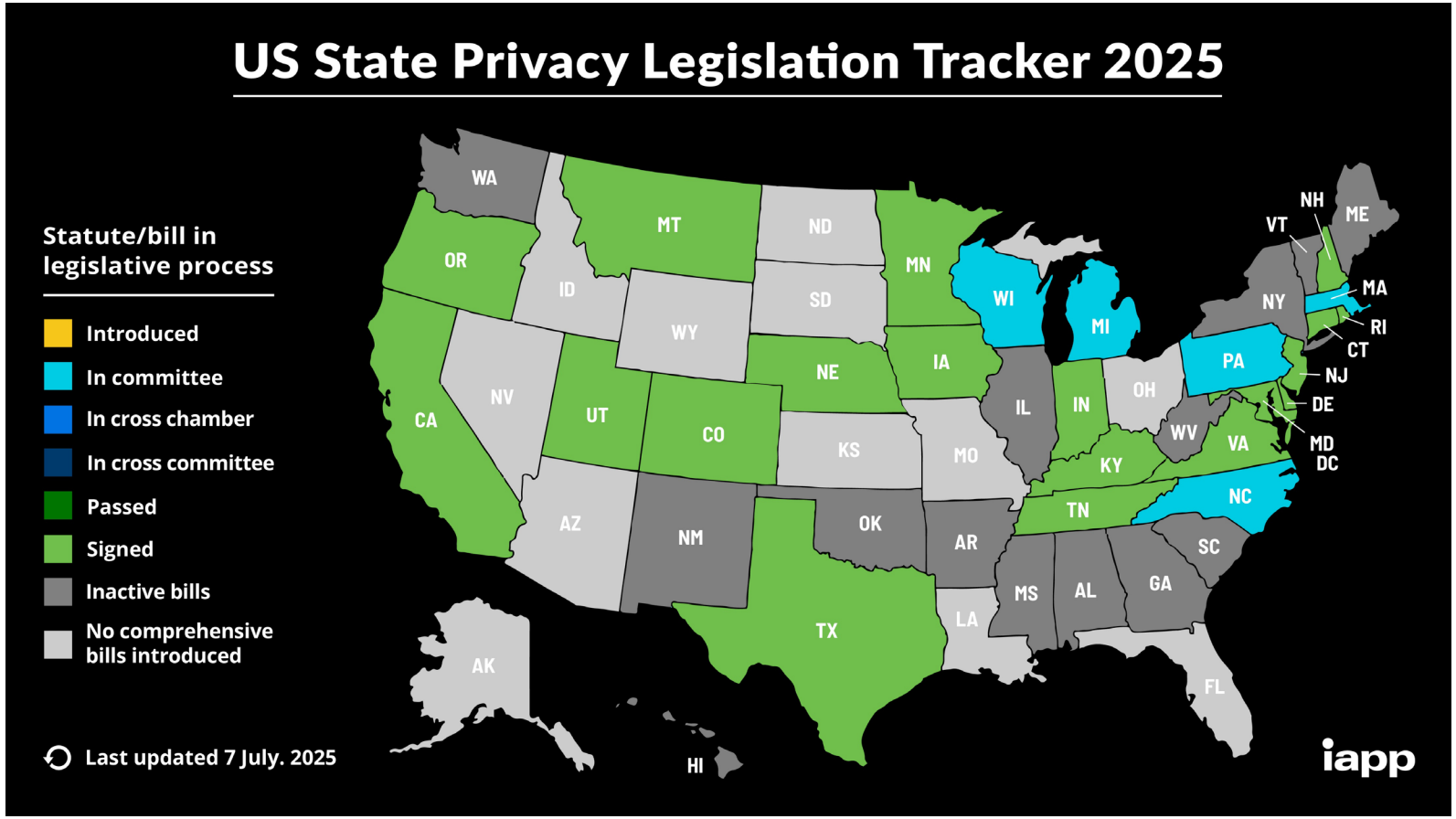
- The shift from voluntary compliance to active enforcement
- The need for proactive risk management and privacy impact assessments
- The role of privacy audits and vendor risk management in enforcement readiness
- AI presents myriad privacy issues, esp. Automated Decision Making (ADMT)
- Time to be Proactive, not just reactive

© 2025 Forvis Mazars, LLP. All rights reserved.

State-Level Privacy Laws Are Expanding Rapidly

It’s Not Just CCPA Anymore

Over 20 U.S. states now have active privacy laws, with new ones like Delaware’s DPDPA, Iowa’s ICDPA, Maryland’s MODPA, and Nebraska’s NDPA taking effect in 2025.



© 2025 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Differences in State Laws

80/20 – Be Aware:

Sensitive Data Definition

Not Universal

- **CT, DE, NJ, MD** include Gender, Financial, Pregnancy, & Health data
- **CA** adds precise geolocation, racial/ethnic origin, & union membership
- **MD** expands to include biometric & neural data

Children's Data Protections

- **CT, CA, OR, MT, NH, MN, NJ, DE, VA**: Require opt-in for targeted ads for ages 13–18
- **MD**: Bans targeted advertising for ages 13–17
- **NY**: Enacted a unique Child Data Protection Act with age-flagging requirements
- **LA, UT, TX** requires notice of age signals for apps

.

Universal Opt-Out Mechanisms (UOOMs)

- Required in **CA, CO, DE, MT, NE, TX, MN, NJ, NH, MD, CT, OR**
- These allow consumers to opt out of data sales/sharing via browser signals or preference settings

Notice & Consent Models

- **Opt-Out Model**: Most states (*e.g.*, VA, CO, TX) follow this
- **Opt-In for Sensitive Data**: Required in CA, CT, CO, MD, & others
- **Strict Consent**: Maryland & Oregon require explicit consent for certain processing activities

AI & Automated Decision Making

- **CO** passed the first AI law in U.S. focusing on transparency & consumer protection
- **CA & MD**: Require disclosures & opt-outs for automated profiling
- **Emerging Trend**: **Over 1,080** AI-related bills have been introduced across all 50 states in 2025 alone.

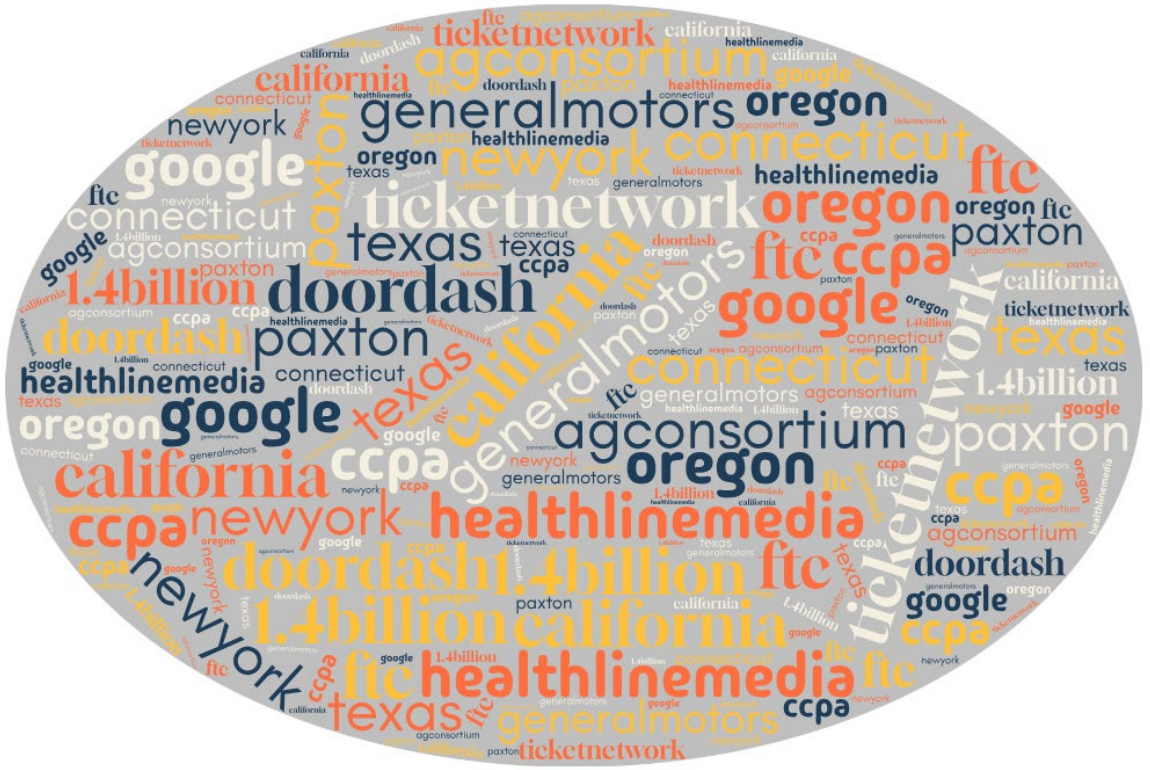
Exemptions

- **B2B & Employee Data**: Exempt in most states except California
- **HIPAA, GLBA, FCRA**: Common exemptions across all laws, but scope & interpretation vary
- **Trend to limit** GLBA exemptions

© 2025 Forvis Mazars, LLP. All rights reserved.

U.S. Privacy Regulators
Proud to Be Active

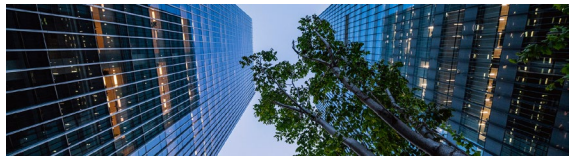
The United States has seen a surge in litigation driven by state-level statutes and consumer empowerment, with nearly 2,500 data privacy lawsuits filed in federal courts in 2024 alone.



- https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-leads-nation-protecting-americans-data-privacy-and-security-big-tech
- https://www.doj.state.or.us/media-home/news-media-releases/attorney-general-rayfield-releases-one-year-report-on-oregon-consumer-privacy-act/
- https://cppa.ca.gov/announcements/2025/20250909.html
- https://oag.ca.gov/news/press-releases/state-privacy-regulators-assemble-attorney-general-bonta-announces-bipartisan
- https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

© 2025 Forvis Mazars, LLP. All rights reserved.

Key 2025 Privacy Actions
Low Hanging Fruit Picked



Privacy Policy

- $85K **Connecticut** AG settlement for privacy notice deficiencies against TicketNetwork.
- The AG's office emphasized the importance of maintaining clear privacy notices that describe consumer rights under the CTDPA.

.

Opt-Out

- $1.55M **CCPA** settlement with Healthline Media related to defective consent management, ineffective cookie opt-outs, and purpose limitation claims.
- Healthline Media failed to allow consumers to opt out of targeted advertising and shared data with third parties without CCPA-mandated privacy protections.

Consent

- $1.4B settlement against Google by **Texas** AG for unlawful tracking and lack of consent.

Geolocation

- Actions by **FTC, Nebraska, Indiana, Arkansas, & Texas** against GM for selling location data.

© 2025 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Too Many Cookies Aren't Baked In
Global Privacy Controls Are Coming

Privacy compliance is entering a phase of heightened enforcement, focused on honoring opt-out requests.

Understand

- **GPC** is a technical specification that allows consumers to signal their privacy preferences, such as opting out of data sales, through their browser settings
- **UOOMs** are mechanisms that allow consumers to opt out of data sales and sharing across multiple platforms and services with a single action

New Compliance Requirements:

- Starting January 1, 2026:
  - Conduct and document risk assessments for selling or sharing personal information
  - Provide explicit, user-facing confirmation when UOOM signals are honored
- Honor GPC by default

Recommendations for Businesses:

- Test, Test, and Retest Regularly

© 2025 Forvis Mazars, LLP. All rights reserved.

Specific Concerns
Understand & Respect the Data

Biometric & Neural Data

- Neural data includes information about brainwaves and other nervous system activities
- Existing and emerging regulations have requirements like:
  - **A written policy** for biometric data retention and **informed consent** from consumers *before collecting* biometric identifiers
  - A written policy for destroying biometric information

3PVM

- GPC and UOOMs need to be coordinated with external partners to guarantee compliance
- Contracts must include robust data protection clauses, and regular audits are essential
- **DOJ Bulk Data Transfer Rule**: Restricts sensitive personal data transfers to foreign adversaries

Children's Data

- The FTC reached a $10 million settlement with Disney over claims of illegal data collection from children
- FTC initiated a Section 6(b) investigation into the effects of AI-powered apps on children and teenagers
- The **California Age-Appropriate Design Code Act (CA AADC)**, requires measures such as setting default privacy controls to a high level, evaluating the impact of algorithms and data collection on children, and providing clear, age-appropriate language in user-facing communications

© 2025 Forvis Mazars, LLP. All rights reserved.

AI Governance Risks & Guidance

ADM; Consent; AI Data Governance; Sensitive Data

ADM

- **Transparency** and Notification Requirements
- Modern privacy laws increasingly require organizations to disclose their use of automated decision-making (ADM) technologies. Privacy policies must specify:
  - What kinds of personal information are used in ADM
  - Which decisions are made solely by ADM

Consent

- Define what constitutes valid consent for AI data processing, aligned with legal requirements
- Use plain language
- Offer Granular and Dynamic Consent Options for specific data uses
- Allow real-time access for users to manage, update, or revoke their consent preferences
- Incorporate visual tools (toggles, sliders) to make consent choices intuitive

AI Governance

- Integrate Consent Management into Data Governance
- Map data flows and inventories to identify where consent is required for AI use
- Automate consent capture and tracking using a Consent Management Platform (CMP)
- Algorithmic Transparency and Accountability Organizations must publish transparency reports and regular audits of consent logs and ADM processes are essential

Sensitive Data

- Biometric and neural data is sensitive personal information, requiring explicit consent and heightened security controls
- States like Colorado and Maryland are tightening rules around facial recognition and fingerprinting
- Implement proper safeguards, to avoid privacy violations, *especially when anonymized data becomes identifiable through cross-referencing*

© 2025 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Upcoming Cyber Reporting Requirements

Companies that process more than 250,000 consumers' personal information and to which the CCPA applies **will need to conduct cybersecurity audits.**

Phased implementation timeline based on 2026 gross revenue:

- More than $100 million by April 1, 2028
- $50 million to $100 million by April 1, 2029
- Under $50 million by April 1, 2030

After initial audit, **annual audits,** for the prior year must be completed by April of the current year.

A cybersecurity audit is far more than a compliance checkbox—it's a strategic tool that strengthens defenses, streamlines operations, and builds stakeholder confidence. When integrated into a comprehensive compliance framework, it helps organizations proactively mitigate risks, avoid regulatory penalties, and prevent reputational and operational fallout.

© 2025 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Cross Functional Commitment

Working together to Reduce Data Risks

Risk Assessments – PIAs

- Why Privacy Impact Assessments Are Essential for CISOs:
  - Identify and Mitigate Privacy Risks Early
  - Ensure Compliance With Expanding Privacy Laws
  - Strengthen Trust and Accountability
  - Support AI Governance and Consent Management

Data Mapping/Inventories

- Why Data Inventories and Mapping Are Essential for CISOs:
  - Enable Regulatory Compliance and Audit Readiness
  - Reduce Security and Privacy Risks
  - Streamline Incident Response and Data Subject Requests
  - Support Effective Data Governance and Resource Allocation

© 2025 Forvis Mazars, LLP. All rights reserved.

Benefits of Privacy Compliance

- Data minimization **reduces storage, processing costs, and breach exposure**
- **Streamlines** international expansion by meeting local privacy standards
- Standardized privacy clauses **simplify** vendor onboarding and cross-border transfers
- Privacy programs build stronger data governance and support AI risk management

© 2025 Forvis Mazars, LLP. All rights reserved.

- Thank you – Questions

© 2025 Forvis Mazars, LLP. All rights reserved.

Contact

Forvis Mazars

Alan Gutierrez-Arana
Principal, Sensitive Data Cybercompliance Leader – IT Risk & Compliance
267.342.1286
alan.gutierrezarana@us.forvismazars.com

Nikole Davenport
Director, Privacy – IT Risk & Compliance
404.272.8439
nikole.davenport@us.forvismazars.com

Diana Ramirez
Manager, Data Privacy – IT Risk & Compliance
213.282.8713
diana.ramirez@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2025 Forvis Mazars, LLP. All rights reserved.