2025 Privacy Overview: How to Ensure Compliance and Reduce Business Risk

Scott C. Hall
Partner

Leeza Arbatman
Associate

Kat Gianelli
Associate

Saachi Gorinstein
Associate

Sabrina Larson
Partner

Hunter Moss
Associate

Coblentz Patch Duffy & Bass LLP

Agenda

- Global and U.S. AI Legal Landscape
- U.S. State Privacy Law Review
- Children's Privacy Update
- Health Privacy Developments
- Overview of Privacy Litigation in 2025
- Privacy Enforcement Actions: Lessons & Takeaways
- Action Items For Businesses

Navigating the Shifting AI Landscape

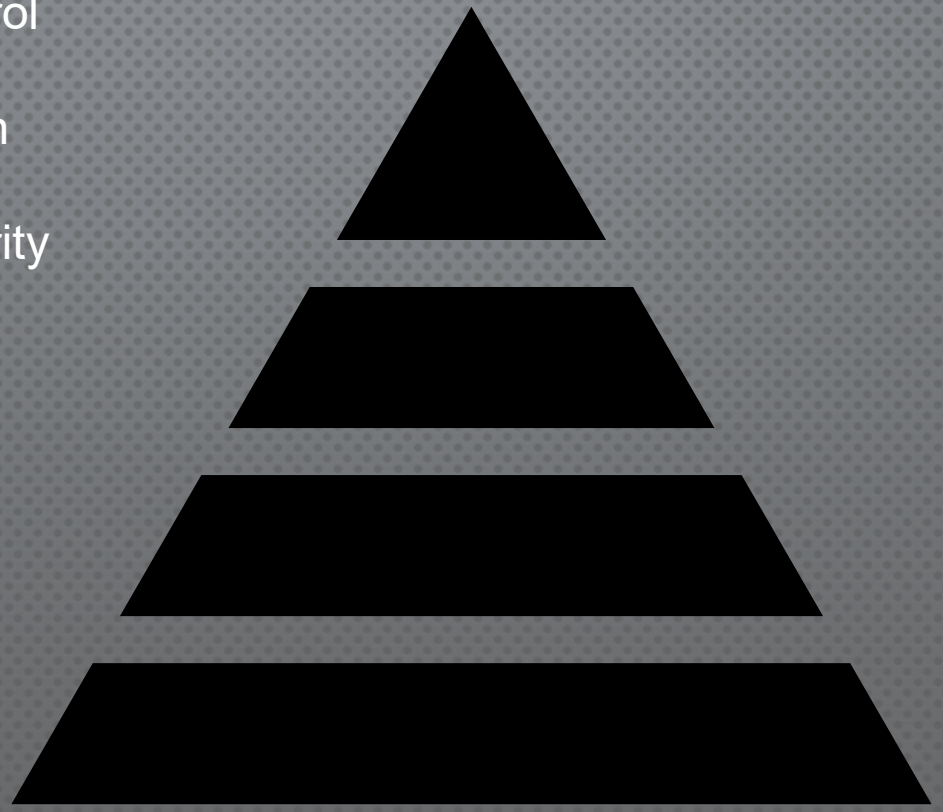
Coblentz
Patch Duffy
& Bass LLP

Navigating the Shifting AI Landscape

EU AI Act

Providers:
- Risk management & quality control
- Validated training data
- Maintain technical documentation
- Ensure human oversight
- Demonstrate accuracy and security

Deployers:
- Use systems as intended
- Conduct risk assessments
- Monitor and log outcomes
- Report serious incidents
- Transparency



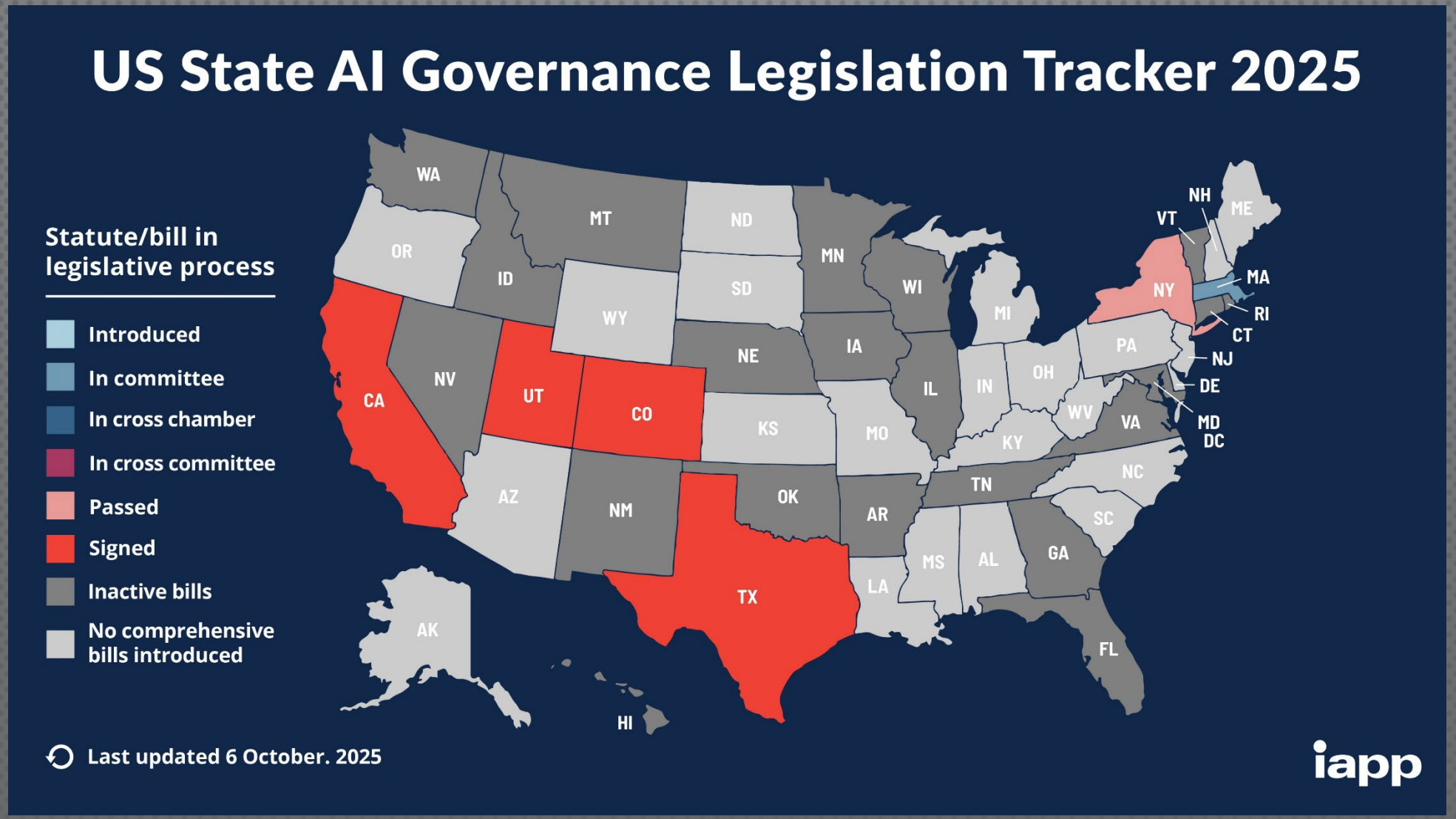
Navigating the Shifting AI Landscape

- Biden Administration Executive Order On Safe, Secure and Trustworthy AI – REPEALED
- Trump Administration – American AI Leadership Order
- Federal Agency AI Oversight/Enforcement
  - FTC
  - EEOC
  - CFPB

Navigating the Shifting AI Landscape

- Transparency in Frontier Artificial Intelligence Act
- New CPPA Regulations
  - Automated Decisionmaking Technology (ADMT)
  - Risk Assessments
  - Cybersecurity Audits
- General AI Training Data Transparency Act
- FEHA Employment AI Regulations

Navigating the Shifting AI Landscape



Source: US State AI Governance Legislation Tracker, IAPP.ORG

Coblentz Patch Duffy & Bass LLP

Navigating the Shifting AI Landscape

- **Compliance Steps for Businesses**
  - Inventory AI Use
  - Conduct Risk and Bias Assessments
  - Enhance Human Oversight of AI Processes
  - Integrate AI and Privacy Governance
  - Monitor Developments

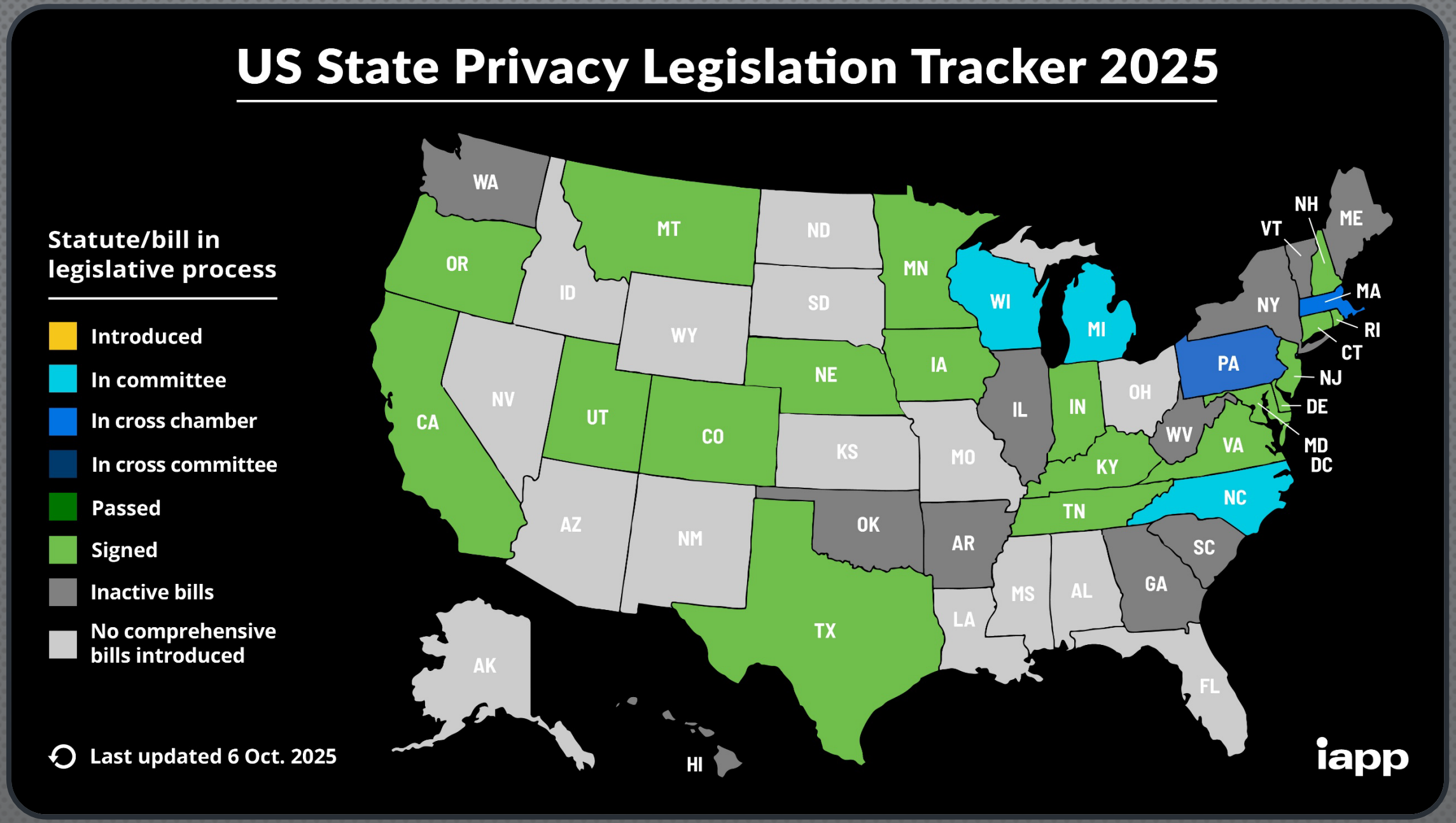
U.S. State Privacy Laws: 2025 Status Update

Coblentz
Patch Duffy
& Bass LLP

Overview of 2025 Privacy Law Landscape

- Eight new states enacted privacy laws: DE, IA, MD, MN, NE, NH, NJ, TN
- Total: **20 states** have passed comprehensive privacy laws
- More than a dozen others considering laws for 2026+
- Businesses face a fragmented, complex compliance environment

US State Privacy Legislation Tracker 2025



Source: US State Privacy Legislation Tracker, IAPP.ORG

Coblentz Patch Duffy & Bass LLP

General Principles of State Privacy Laws

- **Transparency:** provide clear privacy notices to consumers
- **Data minimization:** collect only necessary data
- **Purpose limitation:** use data solely for disclosed purposes
- **Accountability:** ensure proper controls and governance

Consumer Rights Across States

- **Core rights:** access, delete, correct, portability, opt-out
- **Iowa:** limited rights – no correction or profiling opt-out
- **Minnesota:** enhanced transparency and profiling explanations
- **Maryland:** narrower right – categories of third parties disclosed

Opt-Out Preferences & GPC Signals

- All states require opt-out mechanisms
- Some recognize Global Privacy Control (GPC) signals
- New adopters: DE, NE, NH, NJ; MD and MN by end of 2025
- Trend toward interoperability and consumer convenience

Data Protection Impact Assessments (DPIAs)

- Required for "high-risk" processing: targeted ads, profiling, sensitive data
- DE, MD, NE, NH, NJ, TN among those requiring DPIAs
- Encourages proactive privacy risk assessment and mitigation

Sensitive Information: Expanding Definitions

- Broader scope: national origin, gender identity, biometric & financial data
- MD: broad "consumer health data" definition (gender-affirming, reproductive care)
- Processing only if strictly necessary for requested services
- Alignment with health and reproductive privacy trends

Applicability Thresholds of State Laws

- Revenue-based (CA only) vs. data volume thresholds
- Lower thresholds: MD, NH, DE, RI (35k+ residents)
- Broad laws: TX, NE apply to most non-small businesses
- FL: only applies to very large companies ($1B+)

Enforcement of State Privacy Laws

- Primarily enforced by state Attorneys General
- No private right of action (except CA for breaches)
- Cure periods common before penalties apply
- TN introduces National Institute of Standards and Technology (NIST)-based "affirmative defense" for compliance programs

Takeaways for Businesses

- Privacy compliance is now a national business imperative
- Federal law remains uncertain – prepare for continued state patchwork
- Implement scalable, principle-based programs adaptable to change
- Prioritize data mapping, consumer request mechanisms, and GPC recognition

Children's Privacy Update

Coblentz
Patch Duffy
& Bass LLP

Children's Online Privacy Protection Act (COPPA)

- **Who:** Children under 13
- **When:** Deadline to comply is April 22, 2026

COPPA Key Amendments

- Updated parental consent requirements
- Must obtain consent by:
  - Knowledge-based authentication
  - Face verification
  - Text message to parent

COPPA Key Amendments (Continued)

- Limitations placed on data retention and policies
- Written policy must specify:
  - Purpose
  - Specific business need
  - Timeline for deleting

COPPA Key Amendments (Continued)

- Expanded definition of “Personal Information”
- Includes biometric identifiers
  - Fingerprints, handprints, retina patterns, genetic data, voice prints, and facial templates
- Includes Government-issued identifiers
  - Birth certificates, ID cards, passports

COPPA Key Amendments (Continued)

- Enhanced Privacy Notice Requirements
  - State purpose of collecting identifiers
  - Ensure information is not used for unauthorized purpose

COPPA Key Amendments (Continued)

- Written Information Security Program
- Must include:
  - Designated personnel to oversee
  - Annual assessment of risks
  - Implementation of safeguards
  - Testing and monitoring
  - Annual evaluation and updates

Age Appropriate Design Code

- **Who:** All minors under 18 years old
- Broader than COPPA

Age Appropriate Design Code (Continued)

- Focus on design aspects
- High privacy settings by default
- Minimize data collection
- Avoid profiling or geolocation tracking
- Prohibits dark patterns

Takeaways

- Businesses should be mindful of where they collect data and whose data is being collected
- Businesses should update policies to ensure compliance

Health Data Privacy in 2025: Navigating the Current Compliance Landscape

Coblentz
Patch Duffy
& Bass LLP

Introduction: Health Data Privacy at an Inflection Point

- 2025: a turning point for health-data governance
- Expanding regulation across HIPAA, FTC, and states
- Challenge: overlapping frameworks and expectations

HIPAA Reproductive Health Privacy Rule: Paused but Precedent-Setting

- April 2024: Reproductive privacy rule issued
- July 2025: Vacated – APA & authority challenge
- Litigation continues; appeals likely
- Voluntary adoption = proactive risk management

HIPAA Security Rule NPRM: Cybersecurity Comes to the Fore

- Dec. 2024: Proposed Security Rule overhaul
- MFA, encryption, annual reviews
- 24-hour breach notice for business associates
- Align now – OCR treating as expected standard

FTC Health Breach Notification Rule: Extending Beyond HIPAA

- Effective July 2024
- Covers health & wellness apps
- Notify users & FTC within 60 days
- FTC targeting non-HIPAA data handlers

State Laws: A Patchwork of Sensitive Data Frameworks

- WA: Opt-in consent + geofence ban
- CA: CPRA – sensitive wearable data
- TX & FL: Biometric/geolocation focus
- Multi-state harmonization = competitive edge

Intersections and Blind Spots

- Same device, different laws
- HIPAA + State + ADA overlaps
- Data mapping = compliance foundation

Practical Compliance Priorities for 2025

- Risk analyses + data flow mapping
- Update NPPs and privacy notices
- Enhance security + incident response
- Tighten contracts
- Train cross-functional teams

Strategic Implications: The Value of Proactive Privacy

- Privacy = governance + trust
- Regulators reward transparency
- Proactive compliance = competitive advantage

Closing: Partnering for Compliance in 2025 and Beyond

- HIPAA is the base – scope expanding fast
- FTC & state enforcement accelerating
- Partner early to align strategy + compliance

Privacy Litigation Trends

A Privacy Landscape in Flux

Two key statutes of focus:

- Video Privacy Protection Act (VPPA)
- California Invasion of Privacy Act (CIPA)

SB 690: Signals effort to balance

- Consumer privacy
- Overbroad privacy litigation

VPPA: Who is "Identifiable"?

Reasonable Foreseeability Standard

- Info that does not directly reveal person's identity can still lead to liability

Ordinary Person Standard

- Info must allow for identification of person with no specialized tools or knowledge

VPPA: Circuit Split on Who's a "Consumer"

Competing Views Across Circuits:

- Subscribers to free newsletters = consumers.
  Any service containing video qualifies.
  - *Salazar v. NBA* (2d. Cir.)
  - *Gardner v. Me-TV* (7th Cir.)
- Newsletter subscribers ≠ consumers
  - *Salazar v. Paramount* (6th Cir.)
    - Disclosure of viewing data = harm, but no qualifying relationship.

CIPA Developments: Pen Register Claims

- What is a “Pen Register” or “Trap and Trace” Device?
  - A device that captures incoming or outgoing dialing or routing information but *does not capture message contents*.
- Cases Allowing Claims to Survive Past Pleading Stage
  - Focus on collection of identifiable user data and geographic information
- Cases Dismissing Claims at Pleading Stage
  - No reasonable expectation of privacy in routing data; contents not covered by statute
- Positive developments
  - *Mitchener v. CuriosityStream* (N.D. Cal.)
  - *Kishnani v. Royal Caribbean Cruises Ltd.* (N.D. Cal.)

Ninth Circuit Clarifies – and Questions – CIPA

Noteworthy 2025 Ninth Circuit Decision:

- *Guiterrez v. Converse*
  - No evidence of "reading" because of encryption and password protection, even if data *could have* been read by third-party
  - Judge Bybee's concurrence signals CIPA skepticism

SB 690: California's Push to Rein in CIPA Litigation

Purpose

- Creates an exemption for tracking used for a "commercial business purpose."

Scope

- Applies to §§ 631, 632, 637.2, and 638.51.
- Protects analytics, advertising, and personalization tools.
- Prospective only—does not affect pending cases.

Impact

- Website operators and ad-tech gain protection.
- Plaintiffs constrained; harder to bring CIPA lawsuits under the new exemption.

Status

- Passed Senate unanimously. Assembly support is strong.
- Passage likely delayed to 2026, prompting a short-term rush to file new cases before then (especially because it will not apply retroactively).

Conclusion: Privacy Law in Transition

- A shifting legal landscape
  - CIPA and VPPA suits remain prevalent.
  - But case law developments are creating more predictable rules.
  - SB 690 is a clear signal of shifting legislative attitudes.
- Takeaway for Businesses
  - Audit web technologies and data-sharing tools
  - Refresh cookie and privacy disclosures for transparency.
  - Document consent and vendor safeguards.

Proactive steps today will position organizations to weather current litigation trends and thrive once the legal dust settles.

Regulatory Enforcement Actions

Regulatory Enforcement Actions

- Over-verification for Opt-Outs
- Asymmetry in Cookie Management
- Vendor Contract Failures
- Failure to Implement GPC

March 2025
CPPA Administrative Fine: $632,500

Regulatory Enforcement Actions

- Inaccessible Cookie Preferences
- Over-Verification for Opt-Out Requests
- Over-Verification for Verifiable Consumer Requests
- Vendor Technical Failures

May 2025
CPPA Administrative Fine: $345,178

Regulatory Enforcement Actions

- Failure to Honor Opt-Out Requests
- Purpose Limitation Violation
- Vendor Contract Failures
- Deceptive Cookie Banner

July 2025
AG Civil Penalties: $1.55M

Regulatory Enforcement Actions

- Outdated Privacy Policy
- Failure to provide Opt-Out mechanisms/GPC
- Lack of Job Applicant Privacy Notice
- Lack of contracts with ad-tech partners
- Non-Cooperation with regulators

September 2025
CPPA Administrative Fine: $1.35M

Regulatory Enforcement Actions

Common Themes

- Over-Verification for Consumer Requests
- Functionality of Opt-Out Mechanisms
- Symmetry of Choice
- Vendor Oversight & Contracts
- Purpose/Use Limitations
- Cooperation with Regulators
- Don’t Forget Employees and Job Applicants!

Final Takeaways: Action Items For Businesses

- Establish a Comprehensive Privacy & AI Governance Framework
- Strengthen Vendor and Contract Oversight
- Update and Test Consumer-Facing Privacy Infrastructure
- Prioritize Children's and Health Data Compliance
- Enhance Incident Response and Litigation Readiness
- Implement Ongoing Monitoring and Compliance Culture

Questions and Discussion

- Open Floor for Questions

Thank You for Attending

Please direct any questions to Scott Hall and our privacy team.

Scott C. Hall
Partner
shall@coblentzlaw.com

Leeza Arbatman
Associate
larbatman@coblentzlaw.com

Kat Gianelli
Associate
kgianelli@coblentzlaw.com

Saachi Gorinstein
Associate
sgorinstein@coblentzlaw.com

Sabrina Larson
Partner
slarson@coblentzlaw.com

Hunter Moss
Associate
hmoss@coblentzlaw.com

Coblentz
Patch Duffy
& Bass LLP