Coblentz
Patch Duffy
& Bass LLP

2025 Privacy Developments: Action Item Checklist

In 2025, privacy and AI regulation have moved from the sidelines to the center of business risk and strategy. U.S. states are rapidly enacting a patchwork of privacy laws, with new AI laws emerging and expected to increase. Meanwhile, regulators are tightening oversight of automated decision making, children's data, health metrics, and cross-border data transfers. Litigation over online data collection by companies continues to expand under various statutes, including wiretapping and pen register claims under the California Invasion of Privacy Act (CIPA) and claims under the Video Privacy Protection Act (VPPA), resulting in diverging court rulings that send mixed signals to companies regarding privacy compliance. Below is a checklist of action items for businesses to prepare for what is ahead.

Establish a Comprehensive Privacy & AI Governance Framework

- ☐ Inventory all data and AI uses to identify personal data and automated decision-making.
- ☐ Conduct risk and bias assessments; document human oversight, accuracy, and security controls.
- ☐ Maintain governance documentation and monitoring logs to support transparency and compliance readiness.

Strengthen Vendor and Contract Oversight

- ☐ Review vendor contracts for data use limits, breach notice timelines, and cooperation on Data Protection Impact Assessments (DPIAs).
- ☐ Monitor vendors' technical performance, ensuring opt-outs and Global Privacy Control (GPC) signals are honored.
- ☐ Adopt NIST-based or equivalent frameworks to support compliance defenses under state laws.

Update Consumer-Facing Privacy Infrastructure

- ☐ Ensure functional, accessible opt-out mechanisms and symmetry in cookie and preference tools.
- ☐ Refresh privacy policies annually with updated disclosures for employees, applicants, and ad-tech partners.
- ☐ Use layered privacy notices reflecting transparency, purpose limitation, and data minimization.

Prioritize Children's and Health Data Compliance

- ☐ Update policies and practices to meet COPPA amendments and Age-Appropriate Design Code standards.
- ☐ Limit data collection and profiling for minors; prohibit dark patterns.
- ☐ Align health data practices with HIPAA, FTC, and state health privacy frameworks through mapping and security programs.

Enhance Incident Response and Litigation Readiness

- ☐ Update incident response plans for new notification timelines under FTC and HIPAA rules and state laws.
- ☐ Document assessments and policy updates to demonstrate compliance during investigations.
- ☐ Monitor privacy litigation trends (CIPA, VPPA) and assess exposure from tracking or analytics tools.

Implement Ongoing Monitoring and Compliance Culture

- ☐ Track new state and federal developments and adjust programs accordingly.
- ☐ Conduct regular training and audits across teams to reinforce privacy accountability.
- ☐ Promote privacy as a trust and governance priority companywide.

For further information or assistance contact Scott Hall or a member of Coblentz's Data Privacy & Cybersecurity team.

Contacts

Scott Hall
Partner and Chair, Data Privacy & Cybersecurity Group
415.772.5798
shall@coblentzlaw.com
www.coblentzlaw.com

Leeza Arbatman
Associate

415.293.6449
larbatman@coblentzlaw.com
www.coblentzlaw.com

Kat Gianelli
Associate

415.268.0594
kgianelli@coblentzlaw.com
www.coblentzlaw.com

Saachi Gorinstein
Associate

415.268.0515
sgorinstein@coblentzlaw.com
www.coblentzlaw.com

Sabrina Larson
Partner

415.268.0559
slarson@coblentzlaw.com
www.coblentzlaw.com

Hunter Moss
Associate

415.268.0595
hmoss@coblentzlaw.com
www.coblentzlaw.com