Coblentz
Patch Duffy
& Bass LLP

2026 Summer Privacy Webinar Action Item Checklist

Privacy, cybersecurity, and AI compliance continue to move from policy statements to operational controls. Recent enforcement actions and litigation developments underscore that regulators and plaintiffs are focused on whether consumer choices work in practice, whether higher-risk processing is documented, and whether AI, tracking, children's data, sensitive data, and data broker practices are governed with accountability. Below is a practical checklist for businesses following Coblentz's 2026 Summer Privacy Webinar.

Strengthen CCPA Enforcement Readiness

- ☐ Test opt-out, cookie, and Global Privacy Control workflows across websites, apps, accounts, devices, platforms, and vendors.
- ☐ Confirm data minimization, purpose limitation, and notice practices for sensitive data, children/student data, employee/applicant data, and data disclosed to data brokers.
- ☐ Maintain privacy and system records, testing evidence, vendor remediation notes, and other documentation in anticipation of CalPrivacy audits.

Operationalize CCPA Risk Assessments, ADMT, and Cybersecurity Audits

- ☐ Identify high-risk processing, including sale/sharing, sensitive personal information, profiling, automated decision-making technology, and large-scale processing.
- ☐ Complete risk assessments before new high-risk processing begins; update assessments after material changes and at least every three years.
- ☐ Assign owners across legal, privacy, security, product, HR, and data teams; build workflows for 2028 summary reporting and certification obligations.

Address AI Governance

- ☐ Inventory AI tools and vendors; classify uses by risk: internal use, AI-assisted services/deliverables, or AI product development.
- ☐ Adopt internal AI policies and approved enterprise tools; restrict personal, confidential, privileged, and trade secret information in unvetted consumer AI tools.
- ☐ For AI-assisted deliverables and AI products, require human review, IP/license checks, accuracy controls, documentation, transparency, bias/security testing, and clear contract terms.

Prioritize Children, Minors, Health, and Sensitive Data

- ☐ Review online services likely to be accessed by minors for CAADCA obligations, including default privacy settings, age-appropriate notices, age-estimation data, geolocation, and parental-monitoring signals.
- ☐ Harmonize CAADCA, CCPA under-16 sale/share rules, COPPA, health-data frameworks, and state sensitive-data requirements.
- ☐ Evaluate collection, profiling, retention, and sharing of children/student data, health data, precise geolocation, and biometric information for heightened consent and security requirements.

Reduce Litigation, Tracking, and Biometric Risk

- ☐ Audit pixels, cookies, session replay, chat, SDKs, embedded analytics, and ad-tech tools; avoid non-essential tracking before authorization where consent is required.
- ☐ Align consent banners, privacy disclosures, and vendor contracts with actual tracking and data-sharing practices; document technical limits and remediation steps.
- ☐ Maintain biometric notices, written policies, retention schedules, and express consents; monitor BIPA, Texas biometric enforcement, CIPA, VPPA, and CDAFA developments.

Prepare for Data Broker and DROP Obligations

- ☐ Reassess data broker status, including public-record sourcing, aggregation/enhancement practices, "sale" analysis, and whether a direct consumer relationship exists.
- ☐ For registered data brokers, prepare DROP workflows before the August 1, 2026 processing deadline and document deletion exceptions.
- ☐ For non-data brokers, diligence data-broker vendors and update contracts to address downstream deletion, suppression, and data-availability impacts.

Embed Ongoing Monitoring and Compliance Culture

- ☐ Update incident response plans, vendor due diligence, and contract templates for privacy, cybersecurity, AI, and data-broker requirements.
- ☐ Train employees and business owners on privacy rights, AI use, tracking technologies, minors' data, and escalation procedures.
- ☐ Monitor state and federal privacy, cybersecurity, AI, and litigation developments and refresh policies as requirements evolve.

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

Phillip Wiese
Special Counsel

415.268.0502
pwiese@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