CRAVATH

FEBRUARY 2026

Cravath Data Privacy and Security Review

H2 2025

Contents

U.S. Federal – Data Privacy

LEGISLATIVE AND POLICY DEVELOPMENTS

The U.S. remains without a comprehensive federal privacy statute, with the near-term outlook shaped more by state law expansion than federal preemption. The most prominent proposal, the **American Privacy Rights Act of 2024 (APRA)**, was introduced as a discussion draft to create a national baseline for consumer privacy rights and preempt many state laws.

The APRA has not been enacted, so the "compliance fragmentation" problem persists for multi-state businesses managing divergent state laws. This fragmentation extends to litigation and regulation, as companies face compliance questions across multiple legal regimes without a single federal standard.

KEY TAKEAWAYS

- **Plan for continued fragmentation.** Near-term compliance remains driven by the patchwork of state comprehensive privacy laws and sectoral federal regimes.
- **Legislative uncertainty is itself a risk factor.** APRA debates over preemption and private rights of action underscore that any future federal bill could materially reshape, if not altogether displace, existing state frameworks.
- **Retain durable privacy policies.** Regardless of whether a federal bill advances, organizations establish enduring baseline privacy controls (data mapping, minimization, vendor controls, consumer rights operations, incident readiness).

DATA TRANSFERS AND NATIONAL SECURITY

Data transfers are now a national security matter, as highlighted by the Department of Justice's (DoJ) implementation of Executive Order 14117, issued by President Biden in February 2024. This Order aimed to prevent certain countries and "covered persons" from accessing Americans' bulk sensitive personal data and U.S. government-related data. The DoJ's final rule, which took effect on April 8, 2025, established a Data Security Program (DSP) that prohibits or restricts "covered data transactions" and requires due diligence and security controls. Published program materials from the DoJ's National Security Division describe scope, implementation and compliance resources, and indicate the DSP is a lasting control regime, not a one-time initiative.

Importantly, the regime is framed around transaction categories and access pathways instead of relying on traditional concepts of "exports." This framing widens the lens to include vendor and service-provider relationships, remote access, administrative support and onward transfers that could result in foreign access to enumerated sensitive data sets (*e.g.*, health, financial, biometric, geolocation).

The rule is designed to address perceived risks from modern data analytics and AI-enabled exploitation of large datasets, which also explains the policy emphasis on "bulk" thresholds and countries of concern. Overlapping restrictions in this space (including other federal actions targeting sensitive data brokerage and transfers) reinforce a broader theme: cross-border data governance as inseparable from geopolitical and cyber risk management.

KEY TAKEAWAYS

- **Evaluate current data flows for compliance.** Existing transfers and access to data, including among corporate family entities, must be evaluated for compliance with the rule.
- **Vendor diligence must now include "foreign access" risk.** Treat data access pathways (including remote administrative access, support, subcontracting and onward transfers) as priority diligence items for sensitive data sets.
- **Build an EO 14117/DSP "screen" into transaction and contracting workflows.** Identify whether data flows could constitute restricted/prohibited "covered data transactions" and align security controls to the rule's requirements.

U.S. Federal – Cybersecurity

WHITE HOUSE CYBERSECURITY STRATEGY AND FEDERAL POSTURE

In June 2025, the White House issued Executive Order 14306 which amended prior cybersecurity orders, shifting the federal government's approach to private-sector cybersecurity. Instead of expanding mandatory requirements, EO 14306 de-emphasizes prescriptive federal mandates in favor of industry-led standards, voluntary adoption and public-private collaboration.

For companies that develop, sell or deploy software, EO 14306 removes the requirement that federal contractors attest to compliance with the NIST Secure Software Development Framework (SSDF). It also eliminates related centralized validation and enforcement mechanisms. In place of those requirements, EO 14306 directs NIST and the Department of Commerce to develop guidance and best practices grounded in SSDF principles, signaling reliance on market incentives and technical consensus rather than certification regimes.

EO 14306 continues to identify foreign state actors and large-scale cyber threats as national security concerns, preserving federal sanctions and investigative tools. However, it distinguishes government-led threat response from internal private-sector cybersecurity operations, which it suggests are best driven by companies through standards adoption, risk management and commercial pressure rather than federal rulemaking.

EO 14306 also scales back or rescinds certain agency-driven cybersecurity initiatives (including some identity and AI-related pilot efforts), while continuing federal support for technical standards and voluntary programs, such as post-quantum cryptography guidance and the U.S. Cyber Trust Mark for consumer IoT devices. The overall message is one of decentralization: the federal government positions itself as a convener, threat intelligence provider and standard-setter—rather than a direct regulator of private-sector cybersecurity.

KEY TAKEAWAYS

- **Reduced mandate risk, not reduced expectations.** Although companies face fewer executive-order-driven compliance mandates, regulators and counterparties will still expect alignment with recognized cybersecurity standards.
- **Industry standards matter more, not less.** Voluntary frameworks (*e.g.*, NIST SSDF, NIST CSF) will increasingly function as de facto benchmarks in procurement, diligence, and post-incident scrutiny.

FEDERAL CYBERSECURITY REGULATION AND OVERSIGHT

CISA's incident reporting program under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) remains in rulemaking, creating timing uncertainty for compliance planning. CISA has confirmed that reporting obligations are not yet effective. Recent updates to the regulatory agenda suggest the final rule's target has moved to May 2026.

This delay creates two challenges. First, organizations must plan for compliance based on the proposed rule and public statements, knowing key definitions may change. Second, the delay increases the likelihood that organizations will need to navigate overlapping reporting regimes (*e.g.*, from sector regulators or the SEC), increasing the risk of potential liability from inconsistent messaging or conflicting deadlines.

Public reports indicate CISA is considering measures to minimize conflict with other cyber regulations, an acknowledgment of the crowded U.S. reporting landscape. Even with uncertainty around the final rule, companies should prepare for CIRCIA now rather than waiting for its publication.

KEY TAKEAWAYS

- **Regulatory uncertainty persists, but the direction of travel is clear.** Even without a final rule, "critical infrastructure" entities should assume mandatory reporting obligations will be finalized and build compliance capability.
- **Prepare for definitional breadth.** The "covered entity" scope may be broad, requiring organizations near "critical infrastructure" supply chains to watch for indirect effects.

U.S. State – Data Privacy

MULTISTATE ENFORCEMENT AND COORDINATION: EXPANSION OF THE CONSORTIUM OF PRIVACY REGULATORS

State privacy enforcement has matured, marked by the growth of the Consortium of Privacy Regulators. Described by the California Privacy Protection Agency (CPPA) as a bipartisan forum for coordination, the Consortium added Minnesota and New Hampshire in October, expanding to ten regulators. Both states' announcements emphasized coordinated enforcement where laws overlap, while affirming each state's independent authority.

As state agencies develop enforcement teams, investigative tooling and standardized intake of consumer complaints, coordination can shorten the time from initial inquiry to multi-jurisdictional scrutiny. The Consortium's focus on "commonalities" suggests that, where statutes align (*e.g.*, consumer rights mechanisms, opt-out signal recognition, privacy notices, sensitive data treatment), regulators may pursue parallel theories.

This development also interacts with the compliance fragmentation problem: even if laws are not identical, enforcement coordination can spotlight gaps or inconsistencies. The Consortium thus reinforces the need for reliable, cross-jurisdictional evidence of good governance.

KEY TAKEAWAYS

- **Expect more coordinated investigations.** Multistate cooperation increases the likelihood of parallel inquiries, harmonized requests and shared enforcement strategies.
- **Centralize evidence of compliance** to ensure it can be produced efficiently across jurisdictions.

STATE LEGISLATIVE DEVELOPMENTS

Texas Data Broker Act Amendments

Texas has amended its data broker law with two bills (SB 2121 and SB 1343) which took effect on September 1. These changes are significant for companies that previously concluded they were outside the Data Broker Act's scope, as they broaden coverage and adjust compliance mechanics.

A principal change is the expanded definition of "data broker." The statute previously focused on entities with a "principal source of revenue" derived from data broker activities, but the "data broker" definition now includes entities that collect, process or transfer personal data they did not collect directly from the individual. This expanded defition can capture business models where brokering is not the dominant revenue source but where acquisition and downstream transfer of third-party data occurs.

The amendments also strengthen the registration and disclosure framework, reflecting a growing trend of states using broker registration and disclosure regimes to increase transparency around data supply chains and target opaque data acquisition and transfer practices.

The amendments render historical "principal revenue source" analyses less reliable and place greater emphasis on comprehensive vendor and data-flow mapping.

KEY TAKEAWAYS

- **Revisit prior "not a data broker" conclusions.** The new, broader "data broker" definition may pull in entities that collect/process/transfer data they did not collect directly, even if brokering is not the "principal" revenue driver.
- **Revisit contractual relationships.** Ensure vendor agreements and onward transfer terms support Texas compliance representations (and support auditability of downstream uses).

Age-Appropriate Design Codes (AADC)—Continued State Momentum

Age-appropriate design obligations remain a major U.S. state privacy policy theme, even as the legal durability of specific statutes is tested. The most visible model, California's Age-Appropriate Design Code Act (CAADCA), has faced sustained constitutional litigation from industry groups.

Substantively, CAADCA-style proposals tend to focus on product and interface design obligations aimed at minors: risk assessments prior to launching features likely to be accessed by children, default privacy settings for minors, limits on profiling or targeted advertising and restrictions on "dark patterns." The policy logic is driven by a belief that upfront risk management and conservative defaults are more effective.

Even if a specific statute is delayed by litigation, the broader momentum is important for three reasons. First, state legislatures continue to introduce youth-protection frameworks. Second, enforcement agencies can use existing laws to address youth-related design issues. Third, product teams increasingly face design compliance pressure for services with mixed-age user bases that may foreseeably be accessed by minors.

KEY TAKEAWAYS

- **Substance is spreading even where a specific statute is delayed.** Youth-oriented privacy-by-design expectations are spreading and influencing bills, enforcement narratives and platform risk assessments, even where specific statutes are delayed by litigation.
- **Mixed-age services are the core risk zone.** Providers of products that may foreseeably have substantial teen/minor usage should expect scrutiny on defaults, profiling, targeted ads and "dark pattern" allegations.

CALIFORNIA REGULATORY EXPANSION: RISK ASSESSMENTS, AUDITS & ADMT

In September, the California Privacy Protection Agency (CPPA) finalized a major set of regulations implementing the California Privacy Rights Act (CPRA) provisions on risk assessments, cybersecurity audits and automated decisionmaking technology (ADMT). These rules represent the most operationally significant expansion of California's privacy regime since the CPRA became fully enforceable. They will phase into effect starting in 2026, with obligations triggered by activity type, risk level and forthcoming CPPA determinations.

The regulations operationalize statutory concepts that have existed since the CPRA was enacted but had not previously been enforceable. First, the risk assessment framework requires businesses to assess processing activities that present "significant risk" to consumer privacy or security, including processing of sensitive personal information, extensive profiling, targeted advertising and certain uses of automated systems. The CPPA rules specify required assessment elements (*e.g.*, purpose limitation, necessity and proportionality, risk identification and mitigation measures) and require assessments to be documented and retained for potential agency review.

Second, the cybersecurity audit provisions authorize the CPPA to require regular, independent audits for businesses whose processing presents significant risk. While not immediately mandatory for all, the regulations establish the legal framework, core audit elements, and recordkeeping expectations. The CPPA will designate which businesses must conduct audits and how often, mirroring other risk-based regimes and signaling a move toward formalized, auditable security governance.

Third, the ADMT rules are among the most detailed in the U.S., defining ADMT broadly and imposing new transparency, access and opt-out rights for profiling or decisions with significant effects. The rules also introduce pre-use obligations (such as impact assessments), heightened notice requirements and limits on ADMT deployment, bringing California closer to EU-style algorithmic accountability.

Collectively, these regulations move California privacy compliance decisively beyond notice-and-choice toward documented risk governance, aligning enforcement authority with technical, operational and board-level decisionmaking.

KEY TAKEAWAYS

- **California is shifting from reactive enforcement to proactive risk governance.** Documented risk assessments and audit readiness will increasingly define compliance.
- **ADMT obligations will affect far more than "AI companies."** Any use of automated systems for targeting, evaluation or decisionmaking—especially in employment, financial or consumer contexts—can trigger obligations.
- **Plan ahead.** Begin preparing inventories of high-risk processing and automated systems, align internal assessments to CPPA requirements and plan for audit-ready documentation ahead of 2026 effectiveness.

CALIFORNIA ENFORCEMENT HIGHLIGHTS

California Attorney General—Healthline Media Settlement

In July, California's Attorney General announced the largest CCPA settlement to date—a $1.55 million resolution with Healthline Media—underscoring the enforcement focus on sensitive data and modern adtech. The AG's press release frames the settlement as part of a progression of active CCPA enforcement. Allegations centered on Healthline's use of tracking technologies for health-related content and ad monetization and its failure to provide compliant notice and/or honor consumer choices in ways that regulators view as required under the CCPA's "sale/share" and opt-out rules.

The case is notable because "health-related" data risks are not limited to the traditional healthcare provider contexts. Regulators are signaling that websites and apps providing health information can generate sensitive inferences and that sharing those signals with adtech partners can be treated as sharing sensitive personal information—particularly where disclosures, opt-outs or technical controls are deficient. In addition, the public materials emphasize "operational compliance." It is not enough to provide an opt-out mechanism on paper if the company's tag ecosystem and third-party trackers continue to transmit data after a consumer opts out.

Healthline is another strong indicator that California privacy enforcement is converging with broader regulatory attention on tracking technologies, sensitive inference and governance around vendor integrations. Regulators are increasingly comfortable making technical assertions about data flows and treating misalignment between consumer-facing controls and actual practices as an enforcement lever.

KEY TAKEAWAYS

- **Inferences regarding health-related data and adtech remain prime enforcement targets.** Even where data is not classic "medical record" data, regulators are focused on health-related inferences, tracking pixels and downstream sharing.
- **Operationalize opt-outs.** Ensure technical configurations actually stop sale/sharing via third-party tags when consumers opt out.

CPPA—$1.35 million settlement with Tractor Supply Company

In September 2025, the CPPA announced its own largest monetary penalty to-date—a $1.35 million settlement with Tractor Supply Company. The settlement highlights the agency's increasing willingness to seek meaningful monetary penalties and operational remedies for privacy compliance failures. The CPPA's announcement emphasizes two themes: (i) privacy notices and opt-out mechanisms must function as represented and (ii) the extension of privacy governance to job applicants, reflecting California's expanded privacy coverage for employment-related data in recent years.

The CPPA's settlement focused on alleged failures in handling opt-out signals, rights mechanisms that did not stop third-party tracking and deficiencies in service provider/vendor contract structures. The CPPA's settlement also described remedial requirements beyond a fine, such as inventorying tracking technologies and requiring ongoing executive-level compliance certification, signaling an enforcement approach that blends monetary sanctions with governance and assurance mechanics.

This settlement reinforces the expectation that opt-out processes must be technically effective across both first-party systems and third-party tracking integrations. Where a rights workflow suggests sale/sharing has ceased but tracking continues for advertising, regulators may view the issue as both a substantive privacy violation and a transparency/consumer deception issue. The explicit focus on job applicants also serves as a reminder that HR and recruiting platforms (which are often heavily vendor-driven) require the same privacy discipline as consumer-facing programs.

KEY TAKEAWAYS

- **Preference signals are no longer "best efforts".** Regulators expect that opt-out preference signals are honored via technical implementation.
- **Employment/applicant data privacy must be protected.** HR and recruiting workflows need the same rigor as consumer-facing privacy operations.

U.S. State – Cybersecurity

SECTOR-SPECIFIC CYBERSECURITY REGULATION

State-level, sector-focused cybersecurity regulation continues to be led by New York's Department of Financial Services (NYDFS) 23 NYCRR Part 500, which functions as a national bellwether for governance and control expectations in financial services and insurance. The final wave of 2023 amendments to Part 500, which introduced a more tiered, risk-based structure with heightened obligations for "Class A" companies, took effect in November 2025.

Under the amended regime, greater emphasis is placed on formal governance roles, technical control baselines (including multi-factor authentication expectations), incident response planning, documentation and certification processes. Cybersecurity obligations are increasingly judged by operational control performance and the ability to demonstrate that performance through evidence, including inventories of information systems and assets.

As other states and sector regulators continue to harden expectations, Part 500 remains an anchor reference point, and its approach often becomes a proxy for "reasonable" governance expectations in disputes, examinations, and post-incident scrutiny.

KEY TAKEAWAYS

- **Governance is the enforcement fulcrum.** Regulators increasingly look for board and management oversight, documented risk management and auditable control operations.
- **Oversight of third parties is critical.** NYDFS continues its focus on vendor risk management, access controls and security requirements in contracts.

Global Developments

EUROPE

General Court of the European Union upholds EU–U.S. Data Privacy Framework (DPF)

In September, the EU General Court issued its judgment in Case T-553/23 (*Latombe v. Commission*) dismissing a challenge to the Commission's DPF adequacy decision, supporting continued reliance on the DPF for transatlantic transfers at present. The decision reduces immediate uncertainty but does not eliminate longer-horizon litigation/appeal risk, given the history of EU–U.S. transfer frameworks.

European Commission proposes "Digital Omnibus" package

In November, the European Commission published a Digital Omnibus Regulation proposal positioned as a package of technical amendments across a broad set of EU digital laws to reduce burden and increase clarity. If adopted, the package could affect GDPR-adjacent compliance mechanics (including cookie and tracking requirements under the ePrivacy framework) and intersecting cybersecurity obligations (*e.g.*, NIS2) and may also adjust aspects of the EU AI Act timeline and requirements. The Commission's stated framing is "simplification," but the package has also drawn public debate about whether certain changes could weaken digital protections.

KEY TAKEAWAYS

- **EU–U.S. data transfers remain viable—but contingency planning is still prudent.** The General Court's decision supports continued reliance on the Data Privacy Framework, but, given the history of EU–U.S. transfer litigation, companies should maintain fallback mechanisms (*e.g.*, SCC readiness).
- **"Simplification" does not mean deregulation.** The Digital Omnibus package may reduce duplicative or burdensome compliance mechanics, but companies should not expect a rollback of substantive privacy or cybersecurity obligations; changes may instead shift documentation, timing or implementation expectations.

ASIA

India: Digital Personal Data Protection Act (DPDP) becomes operational

In November, India notified the DPDP Rules, which the Indian government described as a "full operationalisation" of the DPDP Act, 2023. The official framework emphasizes a "citizen-centric" approach and reflects familiar core compliance expectations. Core obligations of the DPDP Act include limiting collection to what is necessary for a specified purpose and notification to users of data breaches.

For multinational companies, DPDP should trigger three immediate workstreams: (i) scoping and mapping of India-related data processing; (ii) updates to notices and consent architecture aligned to DPDP concepts; and (iii) incident response readiness that incorporates India's notification expectations and governance requirements.

KEY TAKEAWAYS

- **India has moved from framework to enforcement readiness.** With the DPDP Rules in effect, companies should treat India as an operational privacy jurisdiction, prioritizing consent management, breach notification processes and internal role clarity rather than simply high-level policy alignment.

China: clarified cross-border data transfer measures

China has refined its cross-border personal information transfer framework by completing a long-anticipated "third pathway" alongside security assessments and standard contracts. In October, Chinese regulators released new rules for certifying cross-border transfers of personal data, which took effect January 1, 2026.

Certification provides an additional compliance route for certain categories of transfers, potentially offering operational flexibility for multinational data flows where security assessment thresholds are not triggered or where standard contracts are not optimal. However, China's cross-border regime remains highly technical and documentation-intensive, with a strong emphasis on accountability, security controls and demonstrable compliance. In addition, the system remains dynamic as regulators continue issuing implementing guidance and as enforcement posture evolves. Practically, this reinforces the need for a structured China data transfer governance program.

KEY TAKEAWAYS

- **China's transfer regime is now structurally complete—but still complex.** The addition of a certification route provides flexibility, not simplification; selecting and maintaining the appropriate pathway requires careful consideration.
- **Asia-Pacific compliance requires jurisdiction-specific strategies.** India and China illustrate divergent regulatory philosophies—rights- and consent-driven versus security- and sovereignty-driven—making "one-size-fits-all" regional approaches increasingly difficult to sustain.

Authors

NEW YORK

David J. Kappos
+1-212-474-1168
dkappos@cravath.com

Dean M. Nickles
+1-212-474-1135
dnickles@cravath.com

Sasha Rosenthal-Larrea
+1-212-474-1967
srosenthal-larrea@cravath.com

Carys J. Webb, CIPP/US, CIPP/E, CIPM
+1-212-474-1249
cwebb@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

WASHINGTON, D.C.

Noah Joshua Phillips
+1-202-869-7740
nphillips@cravath.com

CRAVATH

NEW YORK
Two Manhattan West
375 Ninth Avenue
New York, NY 10001
T+1-212-474-1000
F+1-212-474-3700

LONDON
100 Cheapside
London, EC2V 6DT
T+44-20-7453-1000
F+44-20-7860-1150

WASHINGTON, D.C.
1601 K Street NW
Washington, D.C. 20006
T+1-202-869-7700
F+1-202-869-7600

cravath.com