CRAVATH

AUGUST 2026

Cravath Data Privacy and Security Review

H1 2026

Contents

U.S. Federal – Data Privacy

CHILDREN'S PRIVACY: COPPA AMENDMENTS

April marked the culmination of a years-long crusade for expanded children's privacy. April 22 was the compliance deadline for most provisions of the Federal Trade Commission's (FTC's) amended Children's Online Privacy Protection Rule (COPPA), marking over 13 years since COPPA was last updated. Among other changes, these modernizations to COPPA add biometric identifiers to the definition of "personal information," require separate verifiable parental consent for disclosures to third parties (unless the disclosure is integral to the nature of the website or online service), and require operators to maintain a written data retention policy under which children's personal information is retained only as long as reasonably necessary for the specific purpose for which it was collected.

But the COPPA amendments require operators of child-directed and mixed-audience services to revisit more than just their public-facing privacy notices. Companies should confirm that age-screening mechanisms operate consistently across their websites, applications, and connected services; that parental-consent workflows distinguish between internal use and third-party disclosure; and that deletion practices are tied to the purpose for which the data was collected. Operators should also assess whether children's personal information is used in analytics, personalization, recommendations, or AI-related systems.

KEY TAKEAWAYS

- **Update consent and age-screening workflows.** Confirm that age-screening and verifiable parental-consent mechanisms address third-party disclosures and mixed-audience services.
- **Review retention and downstream uses.** Align retention schedules with the stated collection purpose and identify whether children's data is used in advertising, analytics, personalization, or model-training datasets.

AI-ENABLED ADVERTISING CLAIMS AND CONSUMER CONSENT: FTC "ACTIVE LISTENING" SETTLEMENT

In May, the FTC announced proposed settlements totaling $930,000 with Cox Media Group, MindSift, and 1010 Digital Works concerning an AI-powered marketing service, used by the companies, advertised as using conversations captured by consumers' smart devices to target localized advertisements. The FTC alleged that the service did not use voice data and that the companies lacked a reasonable basis for representations that consumers had opted in to the alleged collection and use.

The matters are principally advertising substantiation and deception cases; they do not establish a general duty for purchasers of marketing services to independently validate every technical statement made by every vendor. They do, however, illustrate the risk of perfunctorily repeating vendor claims about AI functionality, source data, or consumer consent without support—whether in consumer-facing or internal materials. The cases are also a reminder that blanket references to "AI" do not vitiate or even mitigate the need to accurately describe a product's actual functionality.

Companies using AI-enabled marketing tools, adtech, or analytics should identify which representations originate with the vendor, determine whether they themselves repeat or rely on those representations, and retain support for material claims. Particular care is warranted where a service is described as using sensitive, unexpected, or difficult-to-observe data sources.

KEY TAKEAWAY

- **Substantiate AI and data source claims.** Marketing and procurement teams should confirm that representations about AI capabilities, source data, and consumer consent are accurate, appropriately qualified, and documented.

CONNECTED PRODUCTS, SENSITIVE LOCATION DATA AND DOWNSTREAM SHARING: GM/ONSTAR ENFORCEMENT

In January, the FTC finalized its order against General Motors and OnStar resolving allegations that the companies collected, used, and sold precise geolocation and driving-behavior data from connected vehicles without adequate notice or affirmative consent. The FTC alleged that certain data was sold to third parties, including consumer reporting agencies, and could be used in insurance-related decisions.

The order requires greater transparency and consumer choice, including affirmative express consent for certain collection, use, and disclosure; access and deletion mechanisms; and options to disable or opt out of certain data collection. It also bars specified disclosures to consumer reporting agencies for five years.

The action's impact goes far beyond connected vehicles, as many connected products collect persistent behavioral, location, or telemetry data that may later be used for purposes remote from the service the consumer originally requested.

For manufacturers and service providers, the principal issue is not just whether data collection appears somewhere in a privacy notice. Companies should assess whether consumers would reasonably understand the volume, sensitivity, and downstream uses of the data; whether consent is obtained at an appropriate point in the product experience; and whether collection and retention remain proportionate to the stated purpose. Contractual restrictions on downstream recipients should also align with the company's public disclosures and technical controls.

KEY TAKEAWAYS

- **Map passive data collection and downstream disclosure.** Identify precise-location and behavioral data collected by connected products, the purposes for which it is used, and each downstream recipient.
- **Test notice, consent, and minimization together.** General disclosure may not be sufficient where sensitive data is collected continuously or used for materially different secondary purposes.

U.S. Federal – Cybersecurity

CYBER STRATEGY FOR AMERICA AND FEDERAL CYBERCRIME POSTURE

In March, the White House released the Cyber Strategy for America, which sets out six policy pillars and emphasizes government coordination, critical-infrastructure resilience, public-private cooperation, technological innovation, and the use of U.S. cyber capabilities. A companion executive action on cybercrime, fraud, and predatory schemes identifies ransomware, malware, phishing, financial fraud, and extortion as priority areas. Programs such as the voluntary U.S. Cyber Trust Mark likewise reflect an effort to make cybersecurity practices more visible in the consumer marketplace.

Neither the Cyber Strategy nor the executive action creates a broad new private-sector cybersecurity regime; rather, their near-term significance is in the details. They may affect agency enforcement priorities, procurement standards, information-sharing initiatives, sanctions activity, and the federal government's willingness to disrupt cybercrime infrastructure. Companies operating in regulated or government-facing sectors should therefore monitor implementation by the agencies and departments with authority over their products, services, or contracts.

The Cyber Trust Mark, by contrast, illustrates a distinct phenomenon: Cybersecurity representations are increasingly becoming customer-facing claims. Manufacturers that participate in labeling or certification programs must ensure that the underlying controls remain accurate over the relevant product life cycle and that marketing statements do not overstate the scope or duration of certification.

KEY TAKEAWAYS

- **Monitor implementation rather than treat the strategy as a new rule.** Track agency actions, procurement requirements, and sector-specific measures implementing the stated federal cybersecurity strategy.
- **Consider customer-facing security signals.** Manufacturers of connected products should assess whether voluntary labeling or certification programs are relevant to their products and sales channels.

CIRCIA RULEMAKING AND INCIDENT-REPORTING READINESS

The Cybersecurity & Infrastructure Security Agency (CISA) continued stakeholder engagement on the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rulemaking during the first half of the year, including a number of revised public town halls and other outreach efforts; a final rule has not yet emerged. The possibility of the final rule's enactment in H2 2026 is a sword of Damocles for many entities implicated in "critical infrastructure," a broadly construed set of businesses.

CIRCIA will sit alongside, rather than replace, the Securities and Exchange Commission (SEC), sectoral, state, and contractual notification requirements. A single event may trigger several analyses involving different definitions, materiality or severity thresholds, deadlines, and recipients. Those obligations may also require decisions before the company has complete technical information or has determined the full operational or financial impact of the incident.

Companies that may be covered should use the remaining implementation period to create new compliance workflows or integrate within existing notification workflows. These workflows should identify internal decision-makers, define escalation criteria, and prepare a reporting matrix that can be updated if and when the final rule is issued. The process should address how legal, security, compliance, and business teams will share information; who has authority to approve a filing; and how the company will document judgments where an incident falls close to a reporting threshold.

KEY TAKEAWAY

- **Do *not* wait for the final rule.** Covered and potentially covered entities should not wait for the final rule to prepare incident escalation workflows. Companies should build reporting playbooks that can handle CIRCIA, SEC, sectoral, state, contractual, and foreign notification triggers as they crystallize.

U.S. State – Data Privacy

STATE PRIVACY COMPLIANCE EXPANDS, WITH LESS UNIFORMITY

Privacy is no longer a game of inches. The U.S. state privacy landscape progressed further in the first half of 2026, with Indiana, Kentucky, and Rhode Island privacy laws becoming effective. In the same window, Oklahoma and Alabama enacted new comprehensive privacy laws with later effective dates, continuing the expansion trajectory. These developments add to the number of state privacy laws that companies must address in their day-to-day operations, including when responding to consumer requests, processing sensitive data, conducting data protection assessments, and managing service providers.

At the same time, the state-law framework is becoming less uniform. Although many of these laws share a common structure, differences in scope, exemptions, cure provisions, consent standards, appeal rights, and consumer request procedures remain relevant. States are also supplementing comprehensive statutes with requirements directed at particular technologies or processing activities.

Kentucky illustrates both developments. Its comprehensive Consumer Data Protection Act became effective January 1, 2026. In April, Kentucky amended that statute to prohibit controllers from collecting automatic content recognition (ACR) data without consumer consent, effective July 1, 2027. ACR data generally includes information about a consumer's viewing history collected through technology embedded in or operated through a smart television or smart monitor that identifies displayed content by analyzing audio or video fingerprints. The amendment therefore imposes a technology-specific requirement that may not be separately identified through a company's standard state privacy law review.

A compliance program built around one model statute, even if the highest common denominator, may require repeated workarounds as additional laws take effect. That approach becomes increasingly difficult to administer over time and creates a risk that rights are handled inconsistently across business units.

A more durable framework centralizes common functions while preserving the ability to apply jurisdiction-specific rules. Companies should also confirm that their systems can identify the consumer's applicable jurisdiction and processing context without collecting more information than necessary. Periodic testing is important; a process that is legally sufficient on paper may fail when implemented across a number of discrete environments.

KEY TAKEAWAY

- **Account for state-specific requirements within common processes.** Centralize operational processes, but preserve the ability to apply state-specific thresholds, deadlines, exemptions, appeal rights, opt-out requirements, and rules triggered by particular product features or technologies.

California Delete Act / DROP

California consumers have been able to submit deletion requests through the state's Data Registration and Opt-Out Platform (DROP) since January. Beginning August 1, registered data brokers must access DROP at least every 45 days, retrieve and process matching requests, delete associated personal information—including inferences, absent an applicable exemption—and report request status through the platform.

DROP changes data broker compliance from a series of individual webforms into an ongoing, centralized process. Registered brokers must be able to match requests to records, apply exemptions consistently, delete information across repositories, and document completion. They must also address data that may be re-acquired after deletion and determine how suppression mechanisms interact with legal or operational retention requirements.

The platform may also expose weaknesses in data lineage and identity resolution. A broker that cannot determine where a consumer's data resides, how it was derived, or which downstream products contain related inferences may have difficulty completing requests consistently. Companies should therefore test DROP workflows against representative data environments rather than assuming that a centralized intake mechanism resolves downstream execution.

Businesses that are not themselves registered brokers should also consider whether vendors or transaction targets fall within the data-broker regime. For example, a company may rely on a data broker for advertising, identity resolution, fraud prevention, or analytics services. The broker's DROP obligations, and its ability to continue providing particular data following a deletion request, may affect those services. Data-broker status should also be considered in Mergers & Acquisitions diligence where a target collects or licenses information concerning consumers with whom it does not have a direct relationship.

KEY TAKEAWAYS

- **Complete DROP implementation before August 1.** Validate request retrieval, matching, deletion, suppression, and status-reporting workflows.
- **Include data broker status in diligence and vendor review.** Companies should identify vendors and transaction targets that may be subject to California's data broker registration and DROP requirements.

U.S. State – Cybersecurity

NYDFS FRONTIER AI GUIDANCE

On May 21, 2026, the New York Department of Financial Services (NYDFS) issued guidance on cybersecurity risks associated with frontier AI models. NYDFS warned that such models may increase the speed and scale with which threat actors identify and exploit vulnerabilities and urged regulated entities to review risk assessments, vulnerability management practices, legacy systems, and material third-party dependencies.

The advisory does not create new legal requirements; rather, it explains how NYDFS expects regulated entities to apply the existing requirements of 23 NYCRR Part 500 in a changing threat environment. In particular, NYDFS noted that AI tools may allow threat actors to identify and exploit vulnerabilities more quickly, shortening the period between the discovery of a vulnerability and attempted exploitation.

NYDFS-regulated entities should consider whether their existing vulnerability management processes account for this shorter period. This task may include reviewing how quickly material vulnerabilities are identified, prioritized, and remediated, and whether compensating controls are available where a vulnerability cannot be promptly remediated. Legacy systems may warrant particular attention if they are difficult to patch or are no longer supported by the vendor.

The advisory also addresses third-party risk. Regulated entities should understand whether critical service providers rely on frontier AI models or may be exposed to AI-enabled attacks, and should factor those risks into diligence and contractual cybersecurity requirements negotiations. The appropriate response is not necessarily a separate AI cybersecurity program, but an update to existing risk assessments and controls where AI escalates the relevant threat or vulnerability.

KEY TAKEAWAY

- **Refresh risk assessments and vulnerability management assumptions.** Document how frontier-model capabilities affect threat scenarios, remediation timing, legacy-system risk, and critical third-party dependencies.

Global Developments

EUROPE

NIS2 and Cyber Incident Reporting Harmonization

In January, the European Commission proposed targeted amendments to the Network and Information Security Directive (NIS2) as part of a broader cybersecurity package. The proposal would simplify jurisdictional rules, streamline the collection of ransomware-related data, and facilitate supervision of cross-border entities through a stronger coordinating role for the European Union Agency for Cybersecurity (ENISA).

The amendments remain a proposal and require action by the European Parliament and Council. Companies should therefore continue to comply with NIS2 as implemented under applicable member state laws and should not treat the proposed amendments as current requirements.

The proposal is nevertheless relevant to multinational companies because one of its objectives is to reduce uncertainty concerning which member state has jurisdiction over a cross-border entity. The proposal may also affect how ransomware information is collected and shared among regulators. These issues arise against a broader background of overlapping European incident reporting obligations. Depending on the company and the incident, reporting may be required under NIS2, Digital Operational Resilience Act (DORA), the General Data Protection Regulation (GDPR), or the Cyber Resilience Act (CRA), and more than one regime may apply.

Companies should identify the legal entities and operations subject to each regime and determine which internal team will coordinate reports where an incident affects several jurisdictions or business lines. A common factual record and coordinated regulator communications may reduce the risk of inconsistent descriptions, even where the applicable reporting standards and deadlines differ.

KEY TAKEAWAYS

- **Track the proposal, mindful that it is not current law …** Maintain compliance with existing member state requirements while preserving flexibility for future jurisdictional and reporting changes.
- **… but continue to align incident reporting across EU and global regimes.** Multinational companies should align approaches across NIS2, DORA, GDPR, the CRA, and U.S. regimes to ensure consistent and timely reporting across jurisdictions.

Cyber Resilience Act Readiness

The EU CRA's first major operational deadline takes place in September, with the enforcement of reporting obligations for actively exploited vulnerabilities and severe incidents affecting products with digital elements.

Reports will be submitted through ENISA's Single Reporting Platform, with an early warning generally due within 24 hours and a fuller notification within 72 hours.

Because the reporting obligation begins before the CRA's principal product security requirements become applicable, manufacturers should not defer implementation until the broader December 2027 compliance date. Companies should first determine which software, hardware, and connected products fall within the CRA and identify the legal entity responsible for the product.

Manufacturers will also need a process for distinguishing reportable vulnerabilities and incidents from ordinary product security issues. In particular, the company must be able to identify evidence that a vulnerability has been actively exploited and determine whether an incident meets the applicable severity standard. Those decisions may need to be made before the company has completed its technical investigation.

Internal procedures should specify how engineering or security personnel will escalate a potentially reportable event, who will approve the report, and how the CRA filing will be coordinated with customer notices, contractual requirements, and reports under other laws. Manufacturers that depend on distributors, importers, or third-party developers should also ensure that relevant information can be provided quickly enough to meet the reporting deadlines.

KEY TAKEAWAY

- **Prepare now for the September 11 reporting deadline.** Identify in-scope products, assign reporting responsibility, and test workflows for rapidly assessing and escalating vulnerabilities and incidents.

UNITED KINGDOM – DATA (USE AND ACCESS) ACT IMPLEMENTATION

Implementation of the United Kingdom's Data (Use and Access) Act (DUAA) continued during the first half of the year. Most of the DUAA's remaining data protection provisions came into force in February, with the requirement for organizations to maintain a data protection complaints procedure commencing in June. The DUAA also changes aspects of subject access requests, automated decision-making, and the Privacy and Electronic Communications Regulations (PECR).

Companies should instead identify the provisions relevant to their operations and update affected procedures, notices, and governance documents.

The new complaints requirement is likely to require the most immediate procedural change for many companies. Organizations should have a process through which individuals can submit data protection complaints, investigate and respond to those complaints, and maintain appropriate records.

Companies should also review existing procedures for responding to subject access requests and determining whether any automated decision-making activities are affected by the amendments. Businesses engaged in electronic marketing or cookie usage and similar technologies should assess the changes to the PECR that apply to their activities.

Multinational entities may continue to use common UK and EU processes where the requirements remain aligned, but they should not assume that an EU GDPR process will address every UK-specific change. A targeted review of existing controls is generally more appropriate than a wholesale rewrite of the company's UK privacy program.

KEY TAKEAWAY

- **Review UK-specific compliance requirements.** Companies with UK operations should review privacy notices, complaints handling, data subject request processes, automated decision-making practices, and cookie / electronic marketing compliance in light of the forthcoming implementation stages.

Theme: Cross-Border Data Transfers

The first half of this year continued the shift from a single privacy law model for cross-border transfers toward overlapping privacy, cybersecurity, and national-security controls. Here, the Department of Justice's (DOJ's) Data Security Program under Executive Order 14117 restricts or prohibits specified transactions that could provide countries of concern (China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela) access to U.S. government-related data or Americans' bulk sensitive personal data. The program became effective on April 8, 2025 and has remained a significant implementation issue for global data access and vendor arrangements during the first half of this year.

Abroad, China's Personal Information Export Certification Measures, which took effect in January, further specified the certification route for certain exports of personal information. The EU's GDPR transfer requirements, including appropriate safeguards and transfer risk analysis where applicable, continue to operate separately. A company transferring or providing access to data across borders may therefore need to consider several regimes, each of which applies different standards.

The relevant analysis is not limited to the physical transfer of a database from one country to another. Remote access by employees or service providers, cloud administration, technical support, and other routine arrangements may allow a person in another jurisdiction to access regulated data. Under the DOJ Data Security Program, the identity and location of the recipient, the volume and type of data, and the structure of the transaction may be relevant. Under the GDPR and Chinese law, different transfer mechanisms, assessments, or approvals may apply.

Companies should therefore identify significant cross-border access arrangements and determine which legal regimes apply before relying solely on standard contractual transfer provisions. Privacy, cybersecurity, procurement, and sanctions or national-security personnel may all need to participate where the same arrangement raises several types of restrictions.

KEY TAKEAWAYS

- **Identify cross-border *access* as well as transfers.** Cross-border reviews should identify remote access, vendor support, employment, investment, and other arrangements that may provide a foreign recipient access to regulated data.
- **Coordinate privacy, cybersecurity and national-security analyses.** Companies should consider privacy transfer rules, localization requirements, and the DOJ Data Security Program together where the same arrangement may implicate more than one regime.

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