Cravath Data Privacy and Security Review

H1 2025

Cybersecurity

EXECUTIVE ORDER ON CYBERSECURITY, SUSTAINING SOME EFFORTS FROM PREVIOUS ADMINISTRATIONS BUT RECALIBRATING OTHERS

In June, President Trump issued a new Executive Order on Cybersecurity, titled Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144. The order in part continues and in part modifies cybersecurity policies established by the Obama and Biden administrations, including by modifying certain rollout timelines and agency responsibilities. In short, the new order adjusts course on federal cybersecurity policy in part to account for newly developed technology and associated best practices. Its implementation in the second half of 2025 and beyond will offer an early signal of how the current administration intends to balance technological innovation with flexibility in managing federal cybersecurity risk. Notable directives include:

- Continuing efforts to implement secure software development, security and operations practices based on NIST Special Publication 800–218 (*Secure Software Development Framework* (SSDF)) and extending associated deadlines for such implementation;
- Updating NIST Special Publication 800–53 (*Security and Privacy Controls for Information Systems and Organizations*) to provide guidance on how to deploy patches and updates securely and reliably;
- Developing and publishing an update to the SSDF, including practices, procedures, controls and implementation examples regarding the secure and reliable development and delivery of software as well as the security of the software itself; Directing the Federal Government to prepare for a transition to cryptographic algorithms that would not be vulnerable to a cryptanalytically relevant quantum computer (*i.e.*, a quantum computer capable of breaking current public-key cryptographic algorithms);
- Managing deployment of AI technology in connection with threat detection and automated cyber defense; and
- Requiring suppliers of consumer Internet-of-Things devices to the Federal Government to certify devices with Cyber Trust Mark labeling.

NIST RELEASES UPDATED INCIDENT RESPONSE GUIDANCE

In April, NIST released Special Publication 800-61 Revision 3, titled "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile" (SP 800-61r3), the first such update in over a decade. SP 800-61r3 is described as a resource on "how to incorporate incident response recommendations into cybersecurity risk management activities in alignment with [the NIST Cybersecurity Framework 2.0]". Based on the six functions of the Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover and Govern), the revised publication models a lifecycle framework for ongoing cybersecurity risk management and incident response. SP 800-61r3 includes a large number of specific recommendations concerning planning and incident response, examples of which include:

- Establishing a standardized method for calculating cybersecurity risk to aid in prioritizing response and recovery efforts and in comparing the estimated and actual impacts of incidents (GV.RM-03);
- Documenting all roles and responsibilities involving cybersecurity incident response in the organization's policies and ensuring that all appropriate individuals are delegated the authority necessary to fulfill their incident response responsibilities (GV.RR-02); and
- Monitoring of personnel activity and technology usage should include detection of anomalous user activity or unusual patterns of activity, authentication and logical access attempts, and the use of deception technology (DE.CM-03).

Taken together, SP 800-61r3 reflects a shift toward embedding incident response within enterprise-wide risk governance, moving beyond reactive procedures to a lifecycle model of cybersecurity resilience and continuous improvement.

CISA ISSUES AI DATA SECURITY GUIDANCE

In April, the Cybersecurity and Infrastructure Security Agency of the United States Department of Homeland Security (CISA), along with the National Security Agency, the Federal Bureau of Investigation and international partners, released guidance titled "*AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems*". The guidance highlights data security practices to ensure the accuracy, integrity and trustworthiness of AI outcomes and outlines key risks that may arise from data security and integrity issues across all phases of the AI lifecycle, from development and testing to deployment and operation. Of particular note, the guidance sets forth a series of 10 best practices to secure data for AI-based systems, including:

- Sourcing reliable data and tracking data provenance, preferably from authoritative sources, and logging how data moves through the AI system;
- Utilizing quantum-resistant digital signatures to authenticate trusted data revisions and prevent tampering by third parties; and

Where possible, leveraging privacy-preserving techniques such as data depersonalization, differential privacy and federated learning from various different limited data sets.

The guidance further illustrates heightened risks posed by models trained on web-scale datasets (*i.e.*, scraped web data, whether curated or autonomously web-crawled), including the ingestion of malicious content or data intentionally "poisoned" with inaccurate information. In short, the guidance provides

a whole-lifecycle approach to securing AI data and addressing the risks associated with the data supply chain, malicious data and data drift.

SEC ESTABLISHES CYBER & EMERGING TECHNOLOGIES UNIT

On February 20, the SEC announced the formation of the Cyber and Emerging Technologies Unit (CETU) to focus on combating cyber-related misconduct and to protect retail investors from bad actors in the emerging technologies space. The new unit replaces the Crypto Assets and Cyber Unit, which was itself formed out of the Cyber Unit in 2022. Key areas of focus include addressing:

- Fraud committed using emerging technologies, such as artificial intelligence and machine learning;
- Use of social media, the dark web or false websites to perpetrate fraud;
- Hacking to obtain material nonpublic information;
- Takeovers of retail brokerage accounts;
- Fraud involving blockchain technology and crypto assets;
- Regulated entities' compliance with cybersecurity rules and regulations; and
- Public issuer fraudulent disclosure relating to cybersecurity.

The creation of the unit marks a shift away from focusing on crypto assets as the predominant emerging technology of concern from an enforcement perspective, and signals a more technology-neutral approach to address threats posed by AI, fraud perpetrated by internet technology, hacking and fraudulent disclosure by issuers concerning cybersecurity practices.

NYDFS AMENDED CYBERSECURITY RULES TAKE PARTIAL EFFECT

As we've previously discussed, New York continues to expand the scope of its cybersecurity regulations under 23 NYCRR 500 ("Part 500") for banks, insurance companies and other companies in the financial services sector. The latest round of amendments, which started going into effect in late 2023, provide additional prescriptive requirements for covered entities with respect to cybersecurity, including enhanced access controls, expanded use of multi-factor authentication and routine risk assessments and further require covered entities to report to the New York Department of Financial Services (NYDFS) any ransomware and extortion payments within 24 hours of such payment.

In accordance with the rollout scheduled in the amendment, new requirements have come into effect for covered entities. As of April 15, 2025, covered entities were required to file annual notices of compliance with cybersecurity requirements (or an acknowledgment of non-compliance along with a remediation timeline) to the superintendent of the NYDFS. In addition, as of May 1, covered entities had to implement (a) annually recurring penetration testing and automated and manual vulnerability scans of information systems, (b) role-based access controls for user accounts (*i.e.*, providing access to minimally required information based on need), (c) risk-based controls designed to protect against malicious code, including by monitoring and filtering web traffic and e-mail and (d) endpoint detection and response systems to monitor anomalous cyber activity.

Additional requirements will come into effect in November. Namely, covered entities will need to use multi-factor authorization for any individual accessing any information systems

of a covered entity, subject to limited exceptions, and will need to have implemented written policies and procedures designed to create and maintain an inventory of the covered entity's information systems.

ENFORCEMENT SNAPSHOT

Early 2025 has seen enforcement across agencies focused not just on cyber-incidents, but also misrepresentations—whether made to regulators or to customers or false representations of cybersecurity compliance made by vendors to government agencies. Some of the most notable actions of the year include:

- In January, the Federal Trade Commission (FTC) brought a complaint alleging violation of Section 5 of the FTC Act against GoDaddy. The FTC claimed, among other things, that the company marketed "award-winning security", while operating a data security program that the FTC described as "unreasonable" for a company of its size and complexity, including failure to adequately inventory and manage its computer assets and security-related software updates, and failure to log security-related events and information. In a May 21 settlement, GoDaddy agreed to desist from making misrepresentations about its security and the extent to which it complies with any privacy or security program sponsored by a government, self-regulatory or standard-setting organization; establish and implement a comprehensive information-security program that protects the security, confidentiality and integrity of its website-hosting services; and hire an independent third-party assessor to conduct reviews of its information security program.
- Also in January, the NYDFS levied a $2 million penalty against PayPal in connection with violations of the Part 500 cybersecurity regulation. The NYDFS found, among other things, that PayPal failed to use qualified personnel to manage key cybersecurity functions and failed to provide adequate training to address cybersecurity risks, leading to sensitive customer information, including social security numbers, being left unredacted and potentially exposed, as well as for failing to implement multifactor authentication controls.
- In February, the Department of Justice (DOJ) reached an $11.25 million settlement with Health Net Federal Services (Centene) (HNFS), resolving allegations that HNFS falsely certified compliance with cybersecurity requirements in a contract with the U.S. Department of Defense (DoD) to administer health benefits program for servicemembers and their families, including by ignoring warnings from third-party security auditors and its own internal audit department regarding cybersecurity risks on HNFS's networks and systems.
- In March, the DOJ reached a $4.6 million settlement with MORSECORP, a cybersecurity ratings platform, for overstating its compliance with cybersecurity standards in violation of the False Claims Act. According to the settlement, MORSECORP failed to, among other things, sufficiently ensure compliance of third-party vendors with respect to security standards imposed by DoD requirements; meet its contractual obligations to implement all cybersecurity controls set forth in NIST Special Publication 800-171; and promptly reconcile its score of 104 against a third-party consultant's

conflicting score of -142—in each case in connection with a review of the DoD's implementation of NIST SP 800-171 controls.

- In April, the SEC charged PGI Global and its founder with a $198 million fraud, alleging that the company misled investors about the capabilities of its purportedly AI-powered cryptocurrency trading platform, including by promising guaranteed returns, and misappropriating more than $57 million of investor funds, including for luxury personal expenses. Criminal charges were also brought against the founder by the U.S. Attorney's Office for the Eastern District of Virginia.
- In May, the DOJ announced an $8.4 million settlement with RTX Corporation and its subsidiaries, including Nightwing Group, stemming from failures to implement NIST Special Publication 800-171 cybersecurity controls on sensitive DoD networks while certifying compliance in violation of the False Claims Act. As part of the settlement, RTX and its subsidiaries agreed to additional monitoring and compliance reporting.

Cybersecurity continues be an important focus for regulators, and enforcement actions may continue to expand beyond cybersecurity incidents to overstatements, omissions and failures to implement controls required under new regulatory frameworks.

State Privacy Developments

CONSORTIUM OF PRIVACY REGULATORS ESTABLISHED TO FURTHER COMMON DATA PRIVACY GOALS

In April, various state regulators, including the California Privacy Protection Agency (CPPA), announced the creation of the "Consortium of Privacy Regulators" (the Consortium), an interstate and bipartisan coalition intended to coordinate investigative strategy and share technological tooling. The Consortium currently includes the CPPA and the attorneys general of California, Colorado, Connecticut, Delaware, Indiana, New Jersey and Oregon.

Under a signed memorandum of understanding, the Consortium committed to facilitating regular interjurisdictional dialogue, sharing enforcement priorities and technical resources and coordinating investigations where statutes overlap.

Although each member state operates under its own comprehensive privacy law, the Consortium emphasizes shared statutory features—such as consumer rights to access, deletion, and opt-out of sale, and parallel business obligations regarding data transparency, security and accountability. According to the CPPA's head of enforcement, the Consortium reflects a shared commitment to curb harms stemming from misuse of sensitive data elements—including health, geolocation and children's data, each a current hot topic in privacy regulation.

The Consortium structure affords regulators greater agility in launching coordinated investigations and enforcement actions, while promoting consistent interpretation of overlapping privacy regimes. Its establishment

marks a shift toward enforcement predictability, as coordinated action may yield clearer expectations—along with heightened scrutiny of inconsistent or lagging compliance programs. Companies operating across these jurisdictions should carefully evaluate their privacy governance frameworks, ensuring alignment with regulatory requirements.

EMERGING LEGISLATIVE THEMES

As comprehensive state privacy frameworks proliferate, recent legislation reflects a deeper focus on particular categories of sensitive data—most notably, precise geolocation information and consumer health data. These categories have emerged as flashpoints in both rulemaking and enforcement, signaling areas of heightened legal exposure for businesses handling such data.

PRECISE GEOLOCATION DATA

States are tightening legal frameworks around the collection and sale of precise location data as enforcement scrutiny ramps up, particularly in the digital advertising ecosystem.

- In March, California's Attorney General Rob Bonta announced an investigative sweep targeting adtech firms, mobile app providers and data brokers that collect or share location data—probing whether they comply with the CCPA's requirements for opt-out mechanisms and prohibitions on the sale/sharing of sensitive geolocation data.
- In May, Colorado (SB 276) amended the Colorado Privacy Act to designate "precise geolocation data" as "sensitive data"—defined as GPS or device-derived location information within approximately a 1,850-foot radius—and now mandates opt-in consent before any sale of such data.
- In June, Oregon (HB 2008) followed suit, imposing a blanket ban on the sale of precise geolocation data (defined as within a 1,750-foot radius) and data of consumers under age 16.

CONSUMER HEALTH DATA

Consumer health data—especially data pertaining to reproductive and sensitive services—is subject to heightened protections via consent, content restrictions, limited retention and geofencing prohibitions.

- In March, Virginia passed an amendment to the VCPA (effective July 1, 2025) with respect to target reproductive and sexual health information, extending obligations beyond HIPAA.
- In January, New York's Health Information Privacy Act was passed by the state legislature and at the time of writing is awaiting the Governor's signature. The Act would prohibit the sale or sharing of health-related app data—including fertility tracker data or geolocation associated with reproductive services—absent express consumer consent and restrict retention unless a permissible purpose applies.
- Throughout 2025, other states, including Connecticut, Nevada, New Mexico, Vermont and Washington, adopted or proposed consumer data

privacy laws embracing geofencing bans, limitations on reproductive health data processing and enhanced confidentiality with respect to this category of data.

THE NEURAL-DATA FRONTIER

Although Colorado and California have been at the vanguard of neural data regulation, bills in Connecticut, Illinois, Massachusetts, Minnesota, Montana and Vermont—though inconsistent in terms of their scope and substantive requirements—attempt to regulate the collection, use and disclosure of neural data. Specifically, the Connecticut, Massachusetts and Illinois bills propose classifying brain-computer-interface outputs as "sensitive data", indicating heightened consent requirements may be on the horizon for neurotechnology.

INTERNATIONAL COLLABORATION

In the first half of the year, the CPPA executed two declarations of cooperation with foreign data privacy regulators, marking another significant step in the CPPA's international privacy collaboration efforts. In January, the CPPA executed a Declaration of Cooperation with South Korea's Personal Information Protection Commission (PIPC); that was followed in April by the Declaration of Cooperation with the United Kingdom's Information Commissioner's Office (ICO).

Under the terms of these declarations, the agencies generally share best practices, investigative methodologies and enforcement lessons; organize regular staff exchanges and bilateral meetings to facilitate dialogue; and explore mechanisms for further collaboration.

These declarations represent the second and third international privacy agreements for the CPPA—following an earlier collaboration with France's CNIL (June 2024)—and reflect the California agency's broader global strategy that includes membership in the Global Privacy Assembly, the Asia Pacific Privacy Authorities and the Global Privacy Enforcement Network.

The declarations do not require enforcement cooperation or data sharing, but clearly signal regulatory alignment in the absence of a federal data protection framework. For businesses operating in these jurisdictions, the agreements signal that regulatory expectations may converge over time, particularly around new frontiers such as automated decision-making, children's data and complex cross-border data flows.

2025 COHORT OF OMNIBUS PRIVACY STATUTES

Several states enacted or brought comprehensive consumer privacy statutes into effect in 2025:

January 1

- Colorado: Mandatory notice of violation and right to cure period expires.
- Connecticut, Texas: Requirement to allow consumers to opt out of processing for purposes of targeted advertising or any sale through opt-out preference signals goes into effect.
- Connecticut: Mandatory right to cure period expires.
- Delaware, Iowa, Nebraska and New Hampshire: Privacy laws go into effect.
- Montana: Data protection assessment requirements apply to processing activities created or generated after this date.

- Montana, New Hampshire: Requirement to allow consumers to opt out of processing for purposes of targeted advertising or any sale through opt-out preference signals goes into effect.
- Minnesota: Data protection assessment requirements apply to processing activities created or generated after this date.
- Texas: Authorized agent provisions, permitting consumers to designate an authorized agent to exercise their data privacy rights, go into effect.

January 15

- New Jersey: Privacy law goes into effect.

July 1

- Colorado: Obligations regarding the collection and processing of biometric data go into effect.
- Delaware: Data protection assessment requirements apply to processing activities created or generated after this date.
- Oregon: Privacy law goes into effect for 501(c)3 tax-exempt organizations.
- Tennessee: Privacy law goes into effect.
- Minnesota: Privacy law goes into effect.

ENFORCEMENT HIGHLIGHTS

In February, the first class action was filed under Washington's My Health My Data Act in February (MHMDA). The class in the case alleged that Amazon's advertising software development kits (SDKs) covertly harvested precise location data and biometric identifiers, then monetized such data and identifiers via targeted advertising and third-party data sales—all without affirmative consumer consent or authorization required under the MHMDA. Although the core allegations are reminiscent of other SDK class actions, the MHMDA angle was a novel one.

In May, Texas Attorney General Ken Paxton secured a record-breaking $1.375 billion settlement with Google in the resolution of two lawsuits first filed in 2022. The claims centered on Google's alleged unlawful tracking of Texans' geolocation, Incognito-mode search history and biometric data (voiceprints, facial geometry) without users' consent—even when location tracking was disabled. Texas asserted these activities were undertaken in violation of Texas's consumer protection statutes. The settlement—the largest single-state privacy enforcement recovery ever against Google—reinforces State AGs' willingness to use their statutory unfair or deceptive acts or practices authorities to pursue significant penalties.

Privacy—Federal

FTC'S FINAL COPPA RULE AMENDMENTS TAKE EFFECT

In June, the FTC's long-awaited amendments to the Children's Online Privacy Protection Rule became effective—the first comprehensive update since 2013 following publication in the Federal Register on April 22 of this year. Operators subject to COPPA must comply with most provisions by April 22, 2026, though certain safe-harbor provisions may require action sooner.

Operators are required to obtain separate verifiable parental consent for disclosures of children's personal information to third parties, including targeted advertising, unless the

disclosure is integral to the service. The definition of "personal information" has been expanded to include biometric identifiers and government-issued identifiers. Among the most enforcement-critical changes:

- Operators must deliver direct parental notices detailing third-party recipients and use purposes, with clear opt-in options separate from general consent.
- Data retention limits now prohibit indefinite storage of children's data, requiring operators to retain only what is reasonably necessary to fulfill the stated purpose.
- A written children's information security program is mandated, with annual risk assessments, designated responsible personnel and safeguards scaled to size, complexity and sensitivity.
- Safe harbor programs must increase transparency by publicly disclosing membership lists, submitting compliance reports and meeting new reporting requirements.

These enhancements reflect the FTC's intensified focus on children's data privacy and establish heightened expectations. Failure to comply may lead to enforcement under both COPPA and broader Section 5 authority, particularly for operators collecting sensitive data from children without proper consent or security controls.

TAKE IT DOWN ACT SIGNED

In May, President Trump signed the bipartisan TAKE IT DOWN Act—the first federal statute criminalizing the nonconsensual publication of intimate images, including AI-generated deepfakes. Covered digital platforms (including public websites, mobile apps and user-generated content services) are now required to implement clearly accessible notice-and-takedown procedures and must remove reported nonconsensual intimate imagery (NCII) within 48 hours of verification.

Failures to comply with such removal obligations are treated as violations of the FTC Act, permitting civil penalties of up to approximately $53,000 per incident; knowingly publishing NCII is a federal criminal offense (with sentencing of up to two or three years' imprisonment for cases in which there are adult or minor victims, respectively).

The law, enforced by the FTC, does not provide for a private right of action; however, it does represent a significant expansion of federal privacy enforcement capabilities and further extends the FTC's regulatory perimeter into algorithmic and generative systems misuse.

Global Bulletin

EUROPE: GDPR REFORM PACKAGE ADVANCES; PROCEDURAL REGULATION AGREED

In June, the Council of the European Union (the Council) and European Parliament (the Parliament) reached a provisional agreement on the long-debated Procedural Regulation (the Regulation)—a legislative measure intended to streamline cross-border enforcement under the General Data Protection Regulation (GDPR). The Regulation, which was initially proposed by the European Commission (EC) in July 2023, addresses longstanding concerns over procedural opacity and inconsistency among supervisory authorities in the context of multi-jurisdictional complaints.

Key components of the Regulation include the establishment of admissibility requirements for complaints, mandatory timelines for key

procedural steps (including a 12-month baseline for standard investigations, with limited extensions for complex cases) and formal rights for complainants and respondents, such as the right to be heard and to access draft decisions. The Regulation also introduces mechanisms to resolve non-contentious cases without triggering the Article 60 cooperation procedure. The European Data Protection Board will be responsible for developing additional implementing guidance, and the Regulation is expected to enter into force in mid-2026, subject to final approval by Parliament and the Council.

In parallel, the EC has continued to advance the GDPR "Simplification Omnibus" initiative, aimed at reducing compliance burdens for small and medium-sized enterprises (SMEs). Among the most significant proposals is an amendment to Article 30(5), which would increase the employee threshold for recordkeeping exemptions from 250 to 750 employees, provided that processing activities are not "high risk" and do not involve special-category data. The EC has stated that the measure is intended to refocus recordkeeping obligations on organizations engaged in complex or sensitive processing, while easing burdens on SMEs—particularly in the digital and health sectors. If adopted, these amendments are expected to save businesses an estimated €400 million annually in compliance costs.

GLOBAL CBPR/PRP CERTIFICATION LAUNCHED

In June, the Global Cross-Border Privacy Rules (CBPR) Forum (the Forum) announced the launch of its Global CBPR and Privacy Recognition for Processors (PRP) certification systems. These programs, which build on the foundational Asia-Pacific Economic Cooperation CBPR system, are intended to facilitate globally interoperable cross-border data flows.

The Forum—whose founding participants include the United States, Japan, South Korea, Singapore, Canada, Mexico, the Philippines, Australia and Taiwan—will administer certification under updated baseline requirements, with a focus on accountability, data minimization and privacy-by-design. The CBPR/PRP systems are voluntary, but businesses seeking certification must be assessed by approved Accountability Agents in their jurisdiction. These certifications are designed to supplement local compliance efforts and streamline vendor risk assessment processes.

The Forum also announced a 2025–2026 implementation roadmap that includes additional guidance for handling sensitive data, children's information and data breach response. These developments position the CBPR/PRP systems as emerging tools in the global privacy landscape, particularly for companies operating across myriad legal regimes and seeking a single certification to demonstrate cross-jurisdictional accountability.

CHINA'S CYBERSPACE ADMINISTRATION ISSUES GUIDANCE ON DATA TRANSFERS

In April and May, the Cyberspace Administration of China issued two rounds of official Q&A guidance clarifying key aspects of China's cross-border data transfer framework under the Personal Information Protection Law (PIPL) and the Data Security Law. The guidance aims to reduce compliance uncertainty for multinational and domestic companies navigating data localization and transfer obligations.

The April Q&A distinguishes between "important data" (subject to security assessments) and "general data" (eligible for standard contractual clauses or certification),

introduces *de minimis* thresholds below which security assessments may not be required and allows certain types of routine transfers to proceed without filing if conducted within a free-trade zone and not involving sensitive data. The May Q&A expands on these principles, offering more granular guidance on filings, assessments and reporting obligations under PIPL.

Although the Q&As do not technically alter any legal requirements under China's existing framework, they do enhance operational clarity—particularly for companies that had delayed implementation pending further rulemaking. Businesses engaged in cross-border transactions or other activities involving Chinese personal data may reconsider whether any simplified pathways are now available to them.

Deep Dive Update – Pixel-Tracking Litigation

PROPOSED AMENDMENT TO THE CALIFORNIA INVASION OF PRIVACY ACT PASSES VOTE IN THE STATE SENATE

As we have previously discussed, plaintiffs in California have recently brought cases under anti-wiretapping provisions of the California Invasion of Privacy Act (CIPA) in connection with the use of tracking pixels and many other online technologies. In June, the California Senate advanced Senate Bill 690 (SB 690), an amendment to CIPA, by a unanimous vote of 35-0. The proposed amendment to CIPA is designed to rein in the proliferation of claims under CIPA brought in connection with online tracking technology by clarifying and tailoring CIPA's scope. Specifically, the CIPA amendment would limit liability for businesses that collect online data for a "commercial business purpose", clarify that certain tracking technologies such as tracking pixels do not constitute "wiretaps" and limit the ability to bring private claims relating to such use of tracking technologies. "Commercial business purpose" is defined to include the processing of personal information that is performed to further a business purpose as defined in subdivision (e) of Section 1798.140 of the California Civil Code (*i.e.*, including in connection with measuring ad impressions, for security purposes, targeted advertising and various other purposes) or that is subject to a consumer's opt-out rights under Section 1798.120, 1798.121 and 1798.135 of the California Civil Code (*i.e.*, the opt-out rights provided under the CPPA and CPRA). SB 690 was designated as a two-year bill, and next will be deliberated by the state Assembly.

FEDERAL COURTS "OPT OUT" OF NOVEL THEORIES OF LIABILITY UNDER CIPA AND OTHER SIMILAR FRAMEWORKS

Over the last several months, multiple federal courts have exhibited skepticism of plaintiffs' theories of liability under CIPA and other similar frameworks in connection with third-party chat APIs, usage of tracking pixels and other similar technologies.

In July, the Ninth Circuit affirmed summary judgment for the clothing retailer Converse in connection with its use of an online customer service chat feature. The plaintiffs claimed that the online chat communications were intercepted by Converse in violation of CIPA Section 631(a). Besides finding that the plaintiffs lacked standing to bring their claim, the court held that the plaintiffs failed to meet their evidentiary burden and provide evidence that a reasonable jury could conclude that the third-party chat provider

"intercepted" the chat content. The decision follows on the heels of a September 2024 dismissal in another case brought against the smart home gym company Tonal in the Southern District of California, in connection with Tonal's use of a third-party API chat feature. In its decision, the court dismissed claims brought under CIPA, finding that the plaintiffs had failed to allege any facts that would constitute a violation of CIPA.

In February, a Central District of California judge rejected claims brought in connection with tracking pixels used by Clearblue, a provider of fertility and pregnancy test products. The plaintiff alleged that she received personalized advertisements on social media after purchasing a fertility product from the Clearblue website. The court granted a motion to dismiss, finding that, in addition to the plaintiff having failed to bring a timely claim within the one-year statute of limitations, Clearblue was not and could not have been an interceptor of the communications made in connection with the purchase because it was the counterparty to those communications.[48]

In May, a judge in the Western District of Pennsylvania found that the presence of a privacy policy link in a webpage footer was sufficient to deem that visitors to the site consented to the data collection activities disclosed by the policy. While this decision was with respect to Pennsylvania's Wiretapping and Electronic Surveillance Control Act, taken together, and, in particular, viewed alongside the proposed CIPA amendment, there appears to be growing momentum to stem the recent tide of tracking technology-related claims being brought under legal frameworks originally targeted at the interception and recording of phone conversations.

NEW YORK

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

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

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

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

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

Callum A.F. Sproule, *CIPT*
+1-212-474-1755
csproule@cravath.com

WASHINGTON, D.C.

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

Cravath, Swaine & Moore LLP

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