Cravath Data Privacy and Security Review

H1 2024

Federal—Privacy

DRAFT AMERICAN PRIVACY RIGHTS ACT DEBUTS: OLD WINE IN A NEW BOTTLE?

On April 7, Senate Commerce Committee Chair Maria Cantwell (D-Wash.) and House Energy and Commerce Committee Chair Cathy McMorris Rodgers (R-Wash.) jointly released the American Privacy Rights Act (APRA), which would establish the first federal data privacy standard; the latest draft was released on June 20. If this sounds familiar, it's because we've been here before—most recently, two years ago with the American Data Privacy and Protection Act (ADPPA), which ultimately failed to pass in the House of Representatives. The APRA faces significant headwinds—in an election year, no less—but its provisions provide significant insight into how Congress is considering key privacy issues.

Key Definitions

Like other comprehensive privacy laws, the APRA assigns a broad definition to "covered data"—"information that identifies or is linked or reasonably linkable" to an individual or device. "Sensitive covered data," which is subject to additional limitations, is also broad, including, notably: calendar and address book data; geolocation information; "private communications"; "video programming viewing information"; and, in the latest draft, an "online activity profile."

"Covered entities" include any for-profit business that has over $40 million in annual revenue or processes over 20,000 consumers' data—other than data brokers, which are always in-scope. The APRA also contemplates a "large data holder" category (over $250 million in revenue and a processor of more than five million individuals).

Finally, the APRA introduces a new concept of "substantial privacy harm," which includes the following categories of harm: $10,000 or more in financial harm; "alleged physical or mental harm to an individual" in a healthcare setting; "highly offensive intrusion" of an individual's reasonable expectation of privacy; or discrimination on the basis of protected characteristics.

Consumer Rights

The APRA creates a familiar set of fundamental privacy rights for consumers—the right to access, correct, delete and export their data. Consumers also have the ability to opt out of the transfer of their data and targeted advertising. The APRA also prohibits transfer of sensitive covered data without affirmative, express consent. Covered entities must provide "clear and conspicuous means" of opting out of transfer and targeted advertising, and of withdrawing previously provided express consent.

Although previous drafts would have provided consumers the right to have "consequential decisions" (related to the provision of housing, employment, credit, education, public accommodations, healthcare or insurance) made by a human instead of artificial intelligence (AI) or machine-learning systems, the June 20 draft removed this provision.

Preemption

Preemption remains one of the most controversial APRA provisions, with many state attorneys general (AGs) exhorting Congress to set a federal floor, rather than a federal ceiling, for privacy protection. Nevertheless, the APRA generally overrides non-sectoral state privacy laws—including laws with arguably stronger consumer protections, such as the California Privacy Rights Act (CPRA)—subject to a limited carveout for remedies. Some state laws, including consumer protection laws, data breach notification laws and laws addressing student and employee privacy, remain intact. Laws offering protection for children's data are only preempted when in conflict with the APRA; states would be able to provide greater protection to children as well.

The APRA exempts "any data subject to" and in compliance with the Gramm-Leach-Bliley Act (GLBA), but does not specify whether state GLBA laws would be similarly preempted.

Enforcement and Remedies

The APRA contemplates multiple mechanisms for enforcement. It directs the Federal Trade Commission (FTC) to establish a new bureau for enforcement; a violation of the APRA constitutes an unfair or deceptive act or practice under the FTC Act. The APRA also authorizes state AGs to bring civil actions upon notification to the FTC.

Most significantly, the APRA includes a private right of action for violations of certain APRA provisions, including with respect to, *inter alia*, data minimization requirements, consumer rights, use of dark patterns and the duty to exercise due diligence in selecting service providers or deciding to transfer covered data to third parties. This private right of action is more expansive than all other federal and state laws currently on the books and will remain a subject of contention as the draft progresses.

Next Steps

The APRA would take effect only 180 days after its passage, presenting a very narrow window for covered entities to come into compliance. That possibility remains on the distant horizon, given the many hurdles the APRA still has to clear. The House Committee on Energy and Commerce planned to mark up the bill on June 27, but the mark-up was canceled just minutes before it was due to begin. The future of the bill remains unclear, particularly in light of Congress' upcoming August recess and the November elections at top of mind.

REAUTHORIZATION OF FISA 702

On April 20, President Biden signed the Reforming Intelligence and Securing America Act, providing a two-year extension for Section 702 of the Foreign Intelligence Service Act (Section 702), the controversial program that permits surveillance of certain communications without a warrant.

The amended legislation expands the definition of electronic communications service providers (ECSPs), entities that may be compelled to assist with surveillance—now including "**any** service provider" with "**access** to equipment that is being or may be used to transmit or store wire or electronic communications," as well as "**custodians**" of such entities. According to the Department of Justice (DOJ), this modification is the result of a 2023 dispute in which the government attempted to get an unnamed communications company to aid in overseas surveillance, but the Section 702 tribunal concluded that the service provider did not qualify as an ECSP. The DOJ has committed to applying the definition "exclusively" to the "extremely small" number of technology companies that provide this type of service.

DEVELOPMENTS IN CHILDREN'S PRIVACY

A rising tide lifts all boats. As momentum reaches an all-time high for federal privacy legislation in general, Congress is also closer than ever to overhauling children's privacy. These attempts to modernize children's online safety are targeted efforts to either amend or supplement the Children's Online Privacy Protection Act of 1998 (COPPA), the key federal law governing the online collection of information from children.

COPPA 2.0

The most significant component of this legislative push is colloquially known as COPPA 2.0. First introduced in this legislative session by Sens. Ed Markey (D-Mass.) and Bill Cassidy (R-La.), S. 1418 (the companion bill, H.R. 7890, was introduced by Reps. Kathy Castor (D-Fla.) and Tim Walberg (R-Mich.)), COPPA 2.0 extends COPPA's applications to teens up to 16 years old. The amendment also imposes a flat ban on targeted advertising to children and the collection of any personal information from children unless the collection is "consistent with the context of the relationship and necessary" to provide a requested transaction, service or product. Most notably, though, COPPA 2.0 would apply not only to operators who have "actual knowledge" that a minor is using their services, but also to operators for whom such knowledge is "fairly implied on the basis of objective circumstances," a significant expansion in potential applicability.

APRA, Title II

Title II of the current APRA revisions includes a pared-back version of COPPA 2.0. The revisions do not raise COPPA's age of majority, nor do they revise the "actual knowledge" standard. COPPA 2.0 advocates have voiced disappointment with the proposal, which Rep. Walberg claimed "has the skin but not the meat and bones" of the standalone bills. Expect additional negotiation surrounding children's privacy protection as the APRA mark-up takes shape.

KOSA

The Kids Online Safety Act (KOSA) has also emerged as a key piece of legislation for children online. KOSA was first introduced in 2022 and reintroduced in 2023. Although President Biden publicly endorsed it in July 2023 ("Pass it, pass it, pass it, pass it, pass it."), the bill is only now advancing to the House Commerce Committee.

KOSA targets the design of online platforms—including social media, video games, virtual reality and online messaging services—requiring that these platforms (regardless of revenue or user numbers) implement safeguards for children under 17, including the ability to limit who can contact them and set time limits. It also imposes a duty of care toward children on these platforms, specific to mental health disorders, compulsive usage, sexual exploitation, the promotion of drugs or controlled substances, deceptive marketing, violence, bullying or harassment.

The current proposal contemplates that the FTC and state AGs would share KOSA enforcement authority.

EXECUTIVE ORDER 14117 AND ANPRM FOCUS ON "BULK DATA TRANSACTIONS"

On February 28, President Biden issued Executive Order (EO) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." Unlike decisions administered by the Committee on Foreign Investment in the United States—which impose limitations on a case-by-case basis—EO 14117 categorically seeks to prevent data brokers from selling U.S. data to entities linked to "countries of concern." In conjunction with EO 14117, on

March 5, the DOJ issued a related advance notice of proposed rulemaking (ANPRM), which begins the rulemaking process required by the EO. The comment period closed on April 19.

Covered Data

EO 14117 regulates two types of data—"U.S. government-related data" and "Americans' bulk sensitive personal data." The former category refers to "sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security." The latter category comprises certain (non-public) personal identifiers, geolocation data, biometrics, human genomic data, and personal health or financial information that could be exploited to identify U.S. individuals or groups. This data must be accessed "in bulk," as further defined by future DOJ regulations. We expect significant focus in the public comment process around what constitutes sensitive data, particularly as AI systems enhance their ability to identify individuals from superficially less-sensitive data sets.

Countries of Concern

The "foreign countries of concern" to which the EO and ANPRM apply include six countries: China (including Hong Kong and Macau); Cuba; Iran; North Korea; Russia; and Venezuela. The EO and ANPRM restrict not only transactions involving these foreign governments, but any entity or individual that "as a legal and practical matter … will place" covered data "within the reach of the[se] countries of concern."

Covered Transactions

The ANPRM uses a risk-based approach to regulate data transactions, either prohibiting them altogether or restricting them if risk can be appropriately mitigated.

The ANPRM describes two prohibited transaction types: data-brokerage transactions between U.S. persons and countries of concern, in which covered data is the subject of a commercial transaction (*e.g.*, sale, licensing, access or similar arrangement); and any transactions involving genomic data. The ANPRM would restrict three types of transactions: vendor agreements; employment agreements; and investment agreements. These restricted transactions would only be permitted with sufficient security controls, based on the National Institution of Standards and Technology (NIST) cybersecurity framework.

The DOJ has indicated that it will scrutinize transactions that do not restrict onward transfer of data to countries of concern, regardless of whether these transfers are known or contemplated as of the initial transaction. Although final rules are still on the distant horizon, companies should begin reviewing existing contractual guardrails to avoid potential compliance pitfalls in the future.

ENFORCEMENT NEWS

FTC Participates in Global Cooperation Arrangement for Privacy Enforcement

On January 17, the FTC announced its entry into the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE), an international multilateral arrangement providing for cooperation, assistance with investigations and sharing of information among privacy authorities. Global CAPE supplements cross-border privacy rules created by the Asian Pacific Economic Cooperation for global participation.

FTC: Health and Location Data Should Be "Simply Off-Limits" for AI

On February 27, FTC Chair Lina Khan said that sensitive personal data related to health, location or web browsing history should be "off limits"

for training AI models. Through enforcement actions related to unfair AI-related practices and rulemaking efforts directed to AI-related frauds and scams, the agency continues to voice concern about AI's potential for consumer harm.

NOTABLE ACTIONS

- *FTC: Avast; InMarket; X-Mode*
  These actions underscore the FTC's focus on how browsing and location data can "paint an intimate picture of a person's life" and reveal impermissibly harmful amounts of sensitive information, including medical histories and religious beliefs. These enforcement actions are the newest in a long chronology of FTC actions—including GoodRx, Premom and Cerebral (below)—involving software development kits (SDKs). For a deeper dive into SDKs, please refer to the "Trending" feature on page 10.
- *FTC: Cerebral, Inc.; Monument, Inc.*
  In addition to imposing a $7 million fine on Cerebral, in April the FTC levied a "first-of-its-kind" prohibition on the telehealth firm, banning it from using any personal or health information for advertising purposes. The proposed order in the Monument action would impose a similar restriction on the alcohol addiction treatment service, limiting it from disclosing health information for advertising and requiring receipt of users' affirmative consent before sharing health information with third parties for any other purpose.

Federal—Cybersecurity

CISA PUBLISHES NPRM ON CYBERATTACK REPORTING REGULATION

On April 4—two years after the enactment of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)—the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) published its Notice of Proposed Rulemaking (NPRM) with respect to CIRCIA cybersecurity incident reporting requirements.

In addition to requiring that covered entities report a ransomware payment within 24 hours, CIRCIA also obliges a covered entity to report "substantial" cybersecurity incidents within 72 hours after such entity reasonably believes an incident has occurred.

CIRCIA focuses on 16 "critical infrastructure sectors," which include communications, energy, defense, healthcare and information technology. The NPRM would apply reporting requirements to *all* entities in these sectors (excepting small businesses). The NPRM would also apply reporting requirements to entities that meet one or more sector-based criteria, including providing essential public health–related services and owning or operating financial services infrastructure.

Although CISA limited reporting obligations to only "substantial" cybersecurity incidents, considerable ambiguity remained as to that term's construction. The NPRM clarifies that any cyber incident must meet at least one impact-based criterion in order to trigger any CISA reporting obligation. These criteria are: a substantial loss of confidentiality, integrity or availability of any IT system or network; a serious impact on safety and resilience of operational systems and processes; a significant disruption in the ability to engage in business or industrial operations or the delivery of goods and services; and any unauthorized access to an IT system or network caused by the compromise of a cloud service provider or supply chain.

The comment period for the NPRM closed on June 3. A final rule is expected in late 2025, and reporting requirements will likely begin in 2026.

For more information, please refer to Cravath's April 8 client alert.

NIST PUBLISHES FINALIZED CYBERSECURITY FRAMEWORK 2.0

On February 26, NIST published the final version of its Cybersecurity Framework (CSF) 2.0—the first major update to the framework since its creation a decade ago.

Recognizing that its policies have served as the gold standard for cybersecurity practices across all sectors and industries, NIST has updated existing CSF 1.1 to encourage broad use. The updated framework includes a new governance pillar, with discussion of roles and responsibilities with respect to establishing and evaluating cyber risk management. CSF 2.0 also includes significantly more implementation guidance than its predecessor—NIST provides a suite of new resources, including step-by-step Implementation Examples for CSF 2.0 objectives and Framework Profiles to indicate cybersecurity priorities for specific sectors and use cases.

DIRECTOR OF THE SEC'S DIVISION OF CORPORATE FINANCE PUBLISHES STATEMENT ON FORM 8-K DISCLOSURES FOR MATERIAL CYBERSECURITY INCIDENTS

On May 21, the director of the Securities and Exchange Commission (SEC)'s Division of Corporation Finance, Erik Gerding, published a statement on the new requirement to disclose material cybersecurity incidents under Item 1.05 of Form 8-K ("Material Cybersecurity Incidents").

The SEC requires that reporting companies disclose incidents that are "determined by the registrant to be material" under Item 1.05. This materiality determination must be made "without undue delay"; after a reporting company determines that an incident is material, it must report such incident within four business days. Out of an apparent overabundance of caution, many reporting companies have chosen to report incidents under Item 1.05 that are still undergoing a materiality determination or that have already been determined to be immaterial.

Noting that the adopting release states that Item 1.05 "is not a voluntary disclosure," Director Gerding urged companies to use other items of Form 8-K, citing Item 8.01 (Other Events) as an example, to report cybersecurity incidents that have not—or have not yet—been deemed material. This approach will minimize the "risk that investors will misperceive immaterial cybersecurity incidents as material, and vice versa," and "will allow investors to more easily distinguish" and "make better investment and voting decisions with respect to material cybersecurity incidents."

Federal Communications Commission (FCC) Cyber Trust Mark

On March 14, the FCC adopted a voluntary framework for labeling wireless consumer Internet of Things (IoT) products, which allows IoT manufacturers that receive FCC approval to display a "U.S. Cyber Trust Mark" on their products. Initially, the program will focus on wireless consumer IoT products—smart devices that are not designed for enterprise or industrial settings, such as home security cameras, smart thermostats, fitness trackers and baby monitors, with at least one Commissioner indicating he would support expanding the program to cover "computers, smartphones, routers and non-consumer devices generally."

Although the FCC oversees the program, applications will be reviewed, and Cyber Trust marks will be authorized, by approved private-sector label administrators. Notably, the framework does not provide a safe harbor, nor does it preempt any state law, to protect IoT product manufacturers from associated liability.

FTC Publishes Advisory on Data Security

On April 17, the FTC's Office of Technology published an advisory, "Security Principles: Addressing Vulnerabilities Systematically." The advisory, which underscores the FTC's view that security must be addressed "systematically, not in ad-hoc or one-off ways," provides concrete guidance for mitigating risks associated with "the most prevalent types of vulnerabilities" that the FTC considers "reasonably foreseeable."

These vulnerabilities (and approaches the FTC recommends to address them) are: cross-site scripting (template rendering systems that default to escaping output); SQL injection (query builders and other application programming interfaces (APIs) that clearly delineate between attacker-controlled data and the structure of a query, and code-scanning tools); and buffer overflows and use-after-free vulnerabilities (memory-safe programming languages, such as Python or C#, rather than C+ or C++).

ENFORCEMENT NEWS

FTC Finalizes Updates to HBNR

Consistent with the FTC's emphasis on sensitive health data as a key enforcement priority, on April 26, the agency voted 3–2 to finalize changes to the Health Breach Notification Rule (HBNR), which broadens the scope of HBNR applicability. The changes go into effect on July 29.

The FTC's changes to the definition of "personal health records (PHR) identifiable information"—to cover, *inter alia*, unique device and mobile advertising identifiers—clarify that entities offering or promoting health-related products or services that are outside the ambit of the Health Insurance Portability and Accountability Act (HIPAA) nevertheless are subject to HBNR requirements. The changes also clarify that breaches subject to HBNR requirements include not only cybersecurity breaches but also voluntary disclosures that were not authorized by a consumer.

As highlighted by the split decision finalizing the changes, tension exists between the desire to have HBNR "keep pace with the rapid proliferation of digital health records"—as Chair Khan and Commissioners Rebecca Kelly Slaughter and Alvaro M. Bedoya wrote—and concerns that the "capacious" definitions would place companies "at the mercy of the [FTC]'s enforcement discretion," as dissenting Commissioners Melissa Holyoak and Andrew Ferguson noted. Given the FTC's increasingly aggressive approach to enforcement regarding non-HIPAA health data, companies should closely watch this space and take proactive steps to address potential compliance shortcomings.

SEC Pursues Enforcement Based on Alleged Cybersecurity Deficiencies After Incident

On June 18, the SEC entered into a settlement with business communications and marketing provider R.R. Donnelley & Sons Co. (RRD) for $2.1 million to resolve charges related to RRD's response to a 2021 ransomware attack. Notably, the SEC alleged that RRD's cybersecurity practices violated the disclosure controls and procedures and internal accounting control provisions of the Securities Exchange Act of 1934 (the Exchange Act). Among other failures, the SEC alleged that (i) RRD's internal policies governing review of cybersecurity alerts and incident response failed to sufficiently identify lines of responsibility and authority, set out clear criteria for alert and incident prioritization, and establish clear workflows for alert review and incident response and reporting; (ii) RRD failed to design effective disclosure-related controls and procedures around cybersecurity incidents to ensure that relevant information was communicated to management to allow timely decisions regarding potentially required disclosure; (iii) RRD failed to design and maintain internal controls sufficient to provide reasonable assurances that access to RRD's assets was permitted only with management's

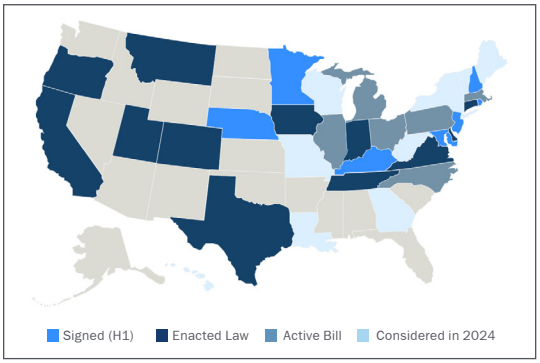
authorization; and (iv) RRD's external and internal security personnel failed to adequately review alerts and take adequate investigative and remedial measures.

The settlement represents a potential expansion of the SEC's ability to directly oversee cybersecurity practices. The allegations in the RRD settlement focused not only on disclosure of the incident, but also purported infirmities in RRD's alert and access management practices purportedly exploited by the threat actors during the cybersecurity incident. Companies should monitor future SEC enforcement actions in this space and regularly test, review and update their cybersecurity policies and procedures.

NOTABLE ACTIONS

- *HIPAA Settlements:* *MedData Inc.*; *Avem Health Partners, Inc.*
  In the wake of 2023's banner year for data breach class actions, several large settlements have been reached in the first half of 2024—including a $7 million settlement for individuals whose information was exposed on GitHub and a $1.45 million settlement for individuals whose information was accessed via a third-party server breach. The Office for Civil Rights (OCR) continues to stress the importance of mitigating cyber threat risks across the sector, particularly given the 256 percent increase in large breaches reported to OCR in the past five years.
- *HIPAA Class Actions:* *ChangeHealthcare*
  Nearly 50 lawsuits brought in the wake of a ransomware attack that rendered ChangeHealthcare's systems inaccessible and leaked sensitive health information of one-third of Americans have been consolidated in the District of Minnesota, the headquarters of its parent company UnitedHealth Group. On May 31, OCR updated its website FAQ to clarify breach notification obligations, explaining that UnitedHealth and Change Healthcare are permitted to notify consumers on behalf of any covered entity affected by the breach.
- *FTC:* *Blackbaud, Inc.*
  On February 1, the FTC entered into a final settlement agreement with software company Blackbaud. The settlement provides additional clarity on appropriate cybersecurity-related safeguards and policies—particularly: encryption of at least sensitive personal data; policies relating to retention (and not just deletion) of personal data; and timely, accurate data breach notifications to consumers.

State—Privacy



H1 2024: TRAIN KEPT A-ROLLIN'

In the wake of a remarkably busy 2023, state legislatures continued to roll up their sleeves in the first half of 2024. As most state legislative sessions are close to adjournment, we reflect on notable developments across the country.

Newly Enacted Laws

At the time of publication, seven states (Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey and Rhode Island) enacted comprehensive privacy laws in the first half of 2024. Although each of these frameworks differs in terms of precise scope and applicability, the laws generally comport with non-California model legislation. None of these laws incorporate a private right of action.

Notable Proposals

Vermont's S. 269 was the most expansive—and most controversial—privacy bill so far this year. S. 269 included controversial age-appropriate design code provisions that have met with legal scrutiny. But more provocative than any other provision was its pioneering private right of action. S. 269 would have permitted citizens to sue for violations of confidentiality of consumer health data, nonconsensual processing of sensitive data and the sale of sensitive data, going beyond limits of the CPRA (limited to data breaches) and Illinois' Biometric Information Privacy Act (limited to biometric information). Ultimately, these provisions proved too contentious to survive—on June 14, Vermont's governor vetoed S. 269, stating it would have made Vermont "a national outlier and more hostile than any other state to many businesses and non-profits." The state legislature did not override the veto.

Although many other proposals largely hew to non-California standard provisions, some contain unusual measures. Rhode Island's law does not apply revenue or processing thresholds—all data controllers are subject to its provisions. Missouri's bill, which ultimately stalled out in committee, would have required compensation for consumers whose personal information was sold—requiring covered businesses to pay consumers 60 percent of what they received for such sales.

Laws Coming Online in H2 2024

Three enacted comprehensive privacy laws are set to come online in the second half of 2024: the Oregon Consumer Privacy Act and the Texas Data Privacy and Security Act (TDPSA) take effect on July 1; Montana's Consumer Data Privacy Act follows on October 1.

Although each of these new laws generally follows Virginia's regulatory model, they also impose new and unique requirements on covered businesses. For example, the TDPSA differs from other state statutes in that it subjects companies outside Texas to the law even if they do not target Texas consumers; it also does not apply a processing or revenue threshold. And the Texas AG has already launched a data privacy and security initiative, providing an early indicator that it intends to be aggressive with respect to enforcement.

CALIFORNIA

CPPA Issues First Enforcement Advisory

On April 2, the California Privacy Protection Agency (CPPA) issued its inaugural enforcement advisory, "Applying Data Minimization to Consumer Requests." The advisory stresses that data minimization is a "foundational principle" of the California Consumer Privacy Act (CCPA), focusing in particular on business responses to consumer requests. According to the CPPA, "certain businesses are asking consumers to provide excessive and unnecessary personal information in response to" data subject requests. The CPPA stresses that the data minimization principle must apply to every step of a covered business's data processing activities, including responses to data subject requests.

The California AG—the CPPA's enforcement counterpart—has heretofore been the more aggressive enforcer of the CCPA. Thus, although this advisory carries no binding legal effect, it is an important shot across the bow. We expect that, as the CPPA commences its own enforcement efforts, data minimization will remain a central focus for the agency.

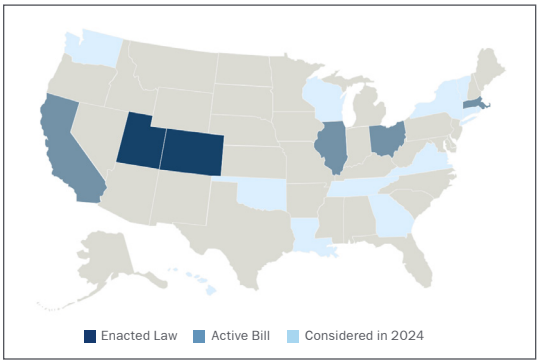
California AG Announces Second Enforcement Action

On February 21, the California AG announced a settlement resolving allegations that food delivery service DoorDash, Inc. violated the CCPA and the California Online Privacy Protection Act (CalOPPA) by participating in a marketing cooperative. DoorDash will be fined $375,000

and is required to, *inter alia*, document its compliance with respect to CCPA-governed sale or sharing of personal information.

In January 2020—the first month that the CCPA was in effect—DoorDash provided non-sensitive consumer information to its marketing cooperative partners in exchange for the ability to advertise to other participants in the cooperative. Although DoorDash did not receive any monetary consideration, the California AG alleged this sharing constituted a "sale" of data under the CCPA definition. Like the Sephora enforcement action that preceded it, the DoorDash settlement serves as a reminder that the California AG will continue to take a particularly aggressive tack on enforcement with respect to the sale or sharing of consumers' personal information.

PRIVATE-SECTOR AI LAWS



Where other technologies have languished for decades without targeted legislation, states have moved with unprecedented speed to respond to AI-related concerns in a number of contexts. Many states began this legislative response several years ago, first turning inward to governmental deployment of AI—establishing task forces to weigh the benefits and risks of deployment and passing laws to curtail or ban certain impermissible uses of AI.

Today, as the generative AI revolution captures the public's attention, state legislatures have turned their focus to the private sector. Typically, cross-sectoral laws that apply to private-sector businesses amend the consumer-protection section of a state's legislative code and are designed to impose guardrails on AI deployment.

Much like international definitions of AI, state law definitions of AI run the gamut. Most 2024 legislation, including Utah's enacted SB 149, focuses on generative AI and synthetic content. Another popular approach is to regulate only automated decision-making systems or systems designed to make "consequential decisions," as in Colorado's enacted SB 24-205. Other bills have proposed applicability to foundation models, dual-use foundation models, frontier models or "general-purpose" systems (*e.g.*, Louisiana's SB118), or only to systems trained on personal data (*e.g.*, Oklahoma's HB 3453).

Although the precise requirements of each law vary significantly, these private-sector laws generally impose similar obligations on developers and deployers of AI. These obligations fall into the following four general categories.

Transparency

Transparency—a fundamental principle in AI governance—undergirds many state AI bills. States operationalize transparency in a variety of ways. Some proposals require public notice of AI governance policies, or labeling of consumer-facing AI systems. Some states would require the disclosure of AI-facilitated decisions or AI-related incidents to consumers or the state government. Finally, some proposals require specific disclosures from developers of AI systems to the users that ultimately deploy them.

AI Governance

Governance is another major component of many state AI bills, but what constitutes good AI governance varies. Proposals include: AI-related policies and risk management programs; risk assessments, impact assessments and rights

assessments; staff training on AI practices and procedures; and the designation of an AI governance officer or a similar "qualified and responsible individual."

Oversight

A smaller number of states propose additional, independent oversight for AI use. Some states (including Utah's SB 149, for AI developers) require proactive pre-disclosure or registration with a governmental entity. A very limited number of states (including, notably, New York) have proposed external review of AI systems and governance programs.

Consumer Rights

Finally, a limited number of states contemplate consumer rights with respect to AI uses. Most states that would impose consumer rights require the avoidance or mitigation of discriminatory impacts of AI systems, or impose a duty of care to protect against algorithmic discrimination. Some state legislation (including Colorado's SB 24-205, for AI deployers) requires an opt-out or appeal mechanism for AI-facilitated decisions.

Many states have meaningfully advanced AI-related legislation in this legislative cycle. Although Congress has considered 108 AI-related bills, none have materialized into law. States stand ready to fill this policymaking gap as this legislative cycle draws to a close—and as we look ahead to 2025.

Global

PRIVACY BULLETIN

China Enacts Final Regulations on Cross-Border Data Flows

On March 22, the Cyberspace Administration of China, the nation's top data regulator, released the final version of its Promoting and Regulating Cross-Border Data Flows (CBDT), with immediate effect. CBDT introduces several key changes to existing policies aimed to streamline cross-border data transfers.

Previously, most data transfers out of China triggered one of three mechanisms: regulator-led security assessments; standard contractual clauses (SCCs); and certification. CBDT introduces higher thresholds for these mechanisms to trigger and also introduces new exemptions (*e.g.*, data necessary for certain contracts; data not personal or "important," as designated by regulators; personal information collected or generated outside of China). CBDT may represent a significant easing of compliance burdens for companies engaging in meaningful cross-border data transfers involving China, but careful consideration of compliance is required as CBDT begins to take effect.

EU AI Act

The Artificial Intelligence Act (AI Act), the first comprehensive AI law, was published in the Official Journal of the EU on July 12 and will come into force on August 1. The AI Act, which establishes obligations for developers and users of AI based on its potential risk and level of impact, is a sweeping, extraterritorial and serious piece of legislation for companies that conduct any business in the European Union.

Although many of the AI Act's provisions do not come into effect until 2026, key provisions—including those covering prohibited AI systems (effective within six months) and those covering generative AI (12 months)—come into force sooner. Given the prevalence of AI in many entities' products and services, companies should begin reviewing their AI policies and practices to quickly move toward compliance.

For more information on the AI Act, please refer to Slaughter & May and Cravath's joint client alert.

Germany's Data Protection Authorities Issue Guidance on AI Implementation in Compliance with GDPR

On May 6, Germany's data protection authorities (DPAs) published guidelines for the implementation of AI in compliance with the European Union's General Data Protection Regulation (GDPR). These guidelines identify key risks associated with AI deployment, chiefly the unlawful processing of personal data and biased data leading to discrimination. The DPAs stressed that entities deploying and developing AI must, in particular, enable data deletion and correction rights as the GDPR prescribes. In addition to warning against AI-related pitfalls, these guidelines advise on best practices for risk mitigation and prevention—chiefly, engaging in impact assessments, AI-use training of employees and similar practices and procedures.

The German DPAs' guidance remains generally in line with other European authorities' views on AI (for example, the French DPA's "how-to" sheets on AI deployment). But these publications are only the beginning of guidance on this emerging topic, and as the technology advances we expect to see further updates to accommodate new developments.

CYBERSECURITY BULLETIN

EU and U.S. Enter into Joint CyberSafe Products Action Plan

On January 30, the EU and the U.S. entered into the Joint CyberSafe Products Action Plan (the Action Plan). The Action Plan builds on commitments President Biden and European Commission President von der Leyen made in October 2023 to cooperate on cybersecurity labeling programs and regulations for IoT devices. The Action Plan aims to further the technical cooperation between the signatories and achieve mutual recognition of cybersecurity requirements for IoT devices, including through shared lexicon and taxonomies with respect to cybersecurity and IoT equipment.

EU Implements Regulation on Voluntary Cybersecurity Certification Scheme

On January 31, the European Commission (EC) adopted the first EU-wide cybersecurity certification framework, the EU Cybersecurity Certification Scheme on Common Criteria (EUCC). Based on the EU Cybersecurity Act, Regulation (EU) 2019/881, the EUCC is intended to standardize the currently fragmented cybersecurity certification scheme for information and communication technology (ICT) across Europe. The implementing regulation details, *inter alia*, the evaluation methodology the EUCC will employ, information necessary for certification and marketing and labeling requirements.

EUCC certificates, which may be issued as soon as January 2025, will be published by the EU Agency for Cybersecurity (ENISA). The EUCC contemplates mutual recognition of similar certifications in foreign jurisdictions (including, potentially, the new U.S. Cyber Trust Mark).

Chile Enacts Cybersecurity Framework Law

On March 26, Chilean President Gabriel Boric signed into law the Framework Law on Cybersecurity and Critical Information Infrastructure (the Framework Law). The Framework Law is intended to ensure continuity of "essential services" in the event of a cyberattack, imposing certain obligations on private and public operators of such essential services. Impacted sectors include healthcare and pharmaceuticals, telecommunications, banking and others as designated by the newly created National Cybersecurity Agency, which is responsible for enforcement. There is no set date for the Framework Law's entry into force.

Trending

SOFTWARE DEVELOPMENT KITS

In 2023, users spent almost 16 billion hours using mobile apps—a 25 percent increase from the previous year and an 86 percent increase since 2020. As mobile apps become an increasingly significant component of the digital ecosystem, regulators both internationally and domestically have focused their enforcement efforts on this type of technology. One particular tool in mobile app development is subject to enhanced scrutiny—the SDK.

An SDK, sometimes known as a "devkit," is a set of components used to build specific functionality for a particular platform, operating system or programming language. These components usually include code libraries, documentation, debugging tools, plug-ins and APIs, among others. Rather than coding a functionality from scratch, developers can license an SDK. Because of their low cost, efficiency and simplicity, SDKs are virtually universal in the mobile app world. To function, SDKs require a significant amount of data from their environment—including personal data under relevant data privacy frameworks.

Although SDKs streamline app creation, they create significant problems with respect to privacy rights and security obligations. Users are frequently unaware that an SDK is being deployed—and if they are, they are likely unable to control what data is collected or how it is used. These problems are not limited to users: developers similarly may be unaware of, or unable to effectively control, the data being collected by SDKs they use. SDKs also present unique security risks: because they are automatically deployed and not removable by a user, they may be more easily exploited by malicious actors. And because they are not easily auditable, vulnerabilities or weaknesses in their deployment may go undetected for a considerable amount of time.

This opacity with respect to data and security has resulted in significant federal enforcement activity from as early as 2016. That year, the FTC kicked off SDK-specific enforcement with its InMobi settlement. Although the mobile advertising network stated it only tracked consumer locations on an opt-in basis, InMobi actually continued tracking network information and, by extension, location data even after customers opted out. This "sidestepping of consumer choice" led to a $4 million civil penalty and required the deletion of all location information that InMobi collected.

Over the past two years, SDKs have been the object of renewed focus for the FTC. In 2023, the FTC's actions against BetterHelp, GoodRx and Premom all prominently featured SDKs. Each of these apps used SDKs to collect sensitive health data from users, but failed to either implement controls on third-party recipients of that data or adequately inform consumers about how data was disseminated using SDKs. This year, in actions against data aggregators InMarket and X-Mode, the FTC noted that "[w]hen a developer incorporates a company's code into their app through an SDK, that developer amplifies any privacy risks inherent in the SDK by exposing their app's users to it."

Private litigants have also entered the SDK fray. Inventive plaintiffs in California have used SDKs as a hook for bringing a case under the anti-wiretapping provisions of the California Invasion of Privacy Act (CIPA)—a statute that has of late been deployed with respect to tracking pixels and many other online technologies. Most notably for SDKs, in *Greenley v. Kochava*, the plaintiff argued that Kochava used an SDK to collect and sell user data without consent. The complaint survived dismissal as the judge interpreted "pen register" under CIPA to include software (including online tracking technologies). If prior novel applications of CIPA are any indicator, we should expect a flurry of activity.

SDKs remain a useful arrow in software developers' quivers, but, given the significant regulatory focus and potential for litigation, SDKs should be carefully and thoughtfully deployed. Entities should be keenly aware of what data SDKs collect, and should be prepared to take responsibility for data disclosed through SDKs within their apps. Companies collecting and processing high-risk or particularly sensitive data, including health data, should take extra precautions to ensure their data-collection practices remain above board.

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

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 10001-1696
T+1-212-474-1000
F+1-212-474-3700

LONDON
CityPoint
One Ropemaker Street
London EC2Y 9HR
T+44-20-7453-1000
F+44-20-7860-1150

WASHINGTON, D.C.
1601 K Street NW
Washington, D.C. 20006-1682
T+1-202-869-7700
F+1-202-869-7600