Cravath Data Privacy and Security Review

H2 2024

PAGES 1-8
Federal—Privacy

PAGES 8-11
Federal—Cybersecurity

PAGES 12-13
State—Privacy

PAGE 14
State—Cybersecurity

PAGES 15-17
Global

Federal—Privacy

SALAZAR V. NBA: HITTING "FAST FORWARD" ON VPPA EXPANSION?

A recent decision in the Second Circuit has continued a trend of court decisions broadening the applicability of the Video Privacy Protection Act (VPPA) to modern technologies. The U.S. Congress adopted the VPPA in 1988 to generally prohibit the disclosure of a consumer's personally identifiable information (PII) collected by video tape service providers to any third party without the consumer's consent. The VPPA's prohibition applies to "video tape service providers", which include any person engaged in the delivery of video tapes "or similar audio-visual materials", whereas "consumers" are defined as any "renter, purchaser or subscriber of goods or services from a video tape service provider".

As we've previously discussed,[1] the adoption of new video distribution technologies has led to successive waves of litigation activity related to the VPPA. While Congress adopted the VPPA with cassette tapes front of mind, courts in the mid-2010s found that internet-based video streaming services and even smart TVs that enable content streaming could also constitute "video tape service providers" under the VPPA. This broad reading prompted the adoption of an amendment to the VPPA in 2013 that expanded the means by which video tape service providers could seek and obtain consumer consent for the sharing of PII.

More recently, a new slew of class actions have been brought alleging violations of the VPPA based on novel theories of the statute's scope. In examining such cases, courts have remained split on how expansively to read the VPPA—including on the basis of whether recipients of free video services constitute "consumers" within the meaning of the statute.

On October 15, the Second Circuit issued a significant ruling in the case of *Salazar v. NBA*. In *Salazar*, the plaintiff alleged that the NBA violated the VPPA by using "tracking pixels" (small pieces of code embedded in a website that collect data on user behaviors) to facilitate Facebook ad-targeting for which the NBA received compensation. In 2023, a district court in the Southern District of New York had dismissed the case for failure to state a claim, finding that the plaintiff was not a "consumer" within the meaning of the statute. The Second Circuit reversed, finding that "consumers" include not just people who rent, purchase or subscribe to a video tape service provider's audiovisual goods or services, but also consumers of *any goods or services* provided by the video tape service provider. To the contrary, a provider need only "dabble" in video distribution to constitute a video tape service provider, and a consumer might be a renter, purchaser or subscriber of any of the provider's other goods or services (even a free newsletter, as was the case in *Salazar*).

1 For more information, please refer to Cravath's July 2023 Privacy and Security Review publication

The Second Circuit's decision in part relied on its observation that, in drafting the VPPA, Congress chose to broadly reference "goods and services" in the "consumer" defined term, deviating from the narrower reference to "prerecorded video cassette tapes or similar audio visual materials" in the "video tape service provider" defined term. Importantly, the Second Circuit's decision does not prohibit a video tape service provider from distributing PII unrelated to its video distribution services (for example, PII collected through the sales of other goods or services). Nevertheless, the Second Circuit's expansive view of the VPPA could have far-reaching implications for businesses engaged in online video distribution, and demonstrates the willingness of some courts to construe congressional intent so as to apply the statute to modern technology.

APRA-CADABRA—A COMPREHENSIVE FEDERAL PRIVACY FRAMEWORK: NOW YOU SEE IT, NOW YOU DON'T

In July of last year, we discussed the introduction of the American Privacy Rights Act (APRA) by Senate Commerce Committee Chair Maria Cantwell (D-Wash.) and House Energy and Commerce Committee Chair Cathy McMorris Rodgers (R-Wash.). The proposed bill would, among other things, establish a comprehensive federal data privacy standard; introduce new definitions for "covered data" and "sensitive covered data"; create consumer rights to access, correct, delete and export their data; and provide mechanisms for enforcement, including expanded authority for the Federal Trade Commission (FTC) and state attorneys general to enforce the statute, as well as a private right of action for certain violations. The abrupt cancellation of a planned markup of the APRA bill by the House Committee on Energy and Commerce on June 27 and the subsequent adjournment of the 118th Congress means that the future of the bill or its future iterations remains uncertain.

The APRA was the latest iteration of the framework originally set forth in the American Data Privacy and Protection Act (ADPPA) (which itself failed to pass in the House prior to the adjournment of the 117th Congress). Some insights into the future of the APRA might be gleaned from criticisms raised by legislators, both regarding the APRA and the ADPPA. In particular, many legislators posed objections to several key provisions that largely fell into three distinct buckets:

- **Federal Preemption:** One major point of contention for both bills was the issue of federal preemption. Some Republicans have argued that the APRA's provisions should largely override state laws, providing a ceiling that would eliminate the administrative costs and burdens placed on interstate commerce brought about by a growing patchwork of state privacy laws. In contrast, some Democrats have stated that federal preemption could undermine states' rights to enforce their own, potentially more stringent, data privacy regulations. This concern is particularly pronounced in states that have already enacted comprehensive data privacy laws, such as California with its California Consumer Privacy Act (CCPA).
- **Private Right of Action and Expanded FTC Authority:** Another significant criticism was the inclusion of a private right of action that would allow individuals to sue companies for violations of APRA. House Republicans contended that this could lead to a surge in litigation, placing a heavy financial and operational burden on businesses, particularly small and medium-sized enterprises that might lack the resources to defend against numerous lawsuits. Others took issue with the expansion of federal power to enforce the APRA. For instance, Senator Ted Cruz (R-Tex.), who will replace Senator Cantwell as Chairman of the Senate Commerce

Committee in the next Congress,voiced opposition to the APRA's grant of "unprecedented power to the FTC to become referees of internet speech".

- **Impact on Innovation:** Many Republican critics of the APRA raised fears that overly restrictive data privacy regulations could hinder the development of new technologies and services—related to compliance costs stemming from both of the foregoing concerns—ultimately putting American companies at a disadvantage in the global market.

These general criticisms have not always been raised cleanly along party lines, but they highlight the complex balancing act that any comprehensive federal data privacy legislation must achieve: protecting consumer privacy while fostering an environment conducive to business growth and innovation, all while navigating contentious questions concerning the allocation of enforcement powers and federalism. As the push toward a comprehensive federal privacy framework continues, expect these flashpoints to impact the final scope of any future legislation.

FTC'S "LOOK BEHIND THE SCREENS" REPORT FINDS STATUS QUO TO BE "UNACCEPTABLE"

On September 19, the FTC released its staff report, "A Look Behind the Screens", which details the data collection and use practices of major social media and video streaming services. The report summarizes information gathered by the FTC in response to orders issued to nine major social media and video streaming companies in December 2020 pursuant to Section 6(b) of the FTC Act. Of note, the information gathered in the report is characterized as "snapshotting" a moment in time between 2019 and 2020. Consequently, it does not reflect changes in company practices or application of new technologies that may have occurred since. In addition, the report generally reflects the views and positions of the current composition of the FTC. The FTC under the second Trump Administration may take a different view. Commissioner Andrew Ferguson, whom the President-elect has designated to be FTC Chair, and his fellow Republican commissioner, Melissa Holyoak, each issued partial dissents from the report (discussed below).

In general, the report examines how major tech companies collect, use, track and derive personal and demographic information; how they determine which ads and other content are shown to consumers; how they apply algorithms or data analytics to personal information; how they measure, promote and research user engagement; and how their practices affect children and teens. The report sets forth three key takeaways:

- **"The Status Quo Is Unacceptable":** The report claims that the amount of data collected by large tech companies is "simply staggering", and includes "what we read, what websites we visit, whether we are married and have children, our educational level and income bracket, our location, our purchasing habits, our personal interests, and in some cases even our health conditions and religious faith". The report further claims that extensive data is collected from both users and non-users of company services and is based on information gathered both on and off company platforms (including through tracking tools and data sets purchased through largely unregulated data brokers).
- **"Self-Regulation Is Not the Answer":** The report states that, in the absence of comprehensive federal legislation on privacy, the use of algorithmic data processing or teen online safety, large tech companies have had "free rein" in their data collection practices. It claims that this environment has resulted in "an enormous ecosystem of data extraction and targeting that takes place largely out of view to consumers".

- **"To Fix the System, Fix the Incentives":** Finally, the report claims that, absent meaningful guardrails, large tech companies are incentivized to develop "ever-more invasive" methods of data collection. The report further claims that unregulated practices were found to have entrenched large tech firms by leveraging informational advantages to stifle new entrants and create walled garden digital ecosystems. The report further claims that unregulated practices were found to have entrenched large tech firms by leveraging informational advantages to stifle new entrants and create walled garden digital ecosystems. The report concludes that business incentives faced by firms generally pit protecting users' privacy against monetization of data.

The report states that companies process and apply collected information for targeted advertising, content recommendations and user engagement analysis, as well as to direct business strategy. The report claims that companies were found to extensively share collected data with affiliates and third parties. In many cases, data is processed using algorithms and artificial intelligence (AI) tools. Data collection minimization, retention and deletion policies were found to vary across companies but were generally found to be deficient, and in many cases data deletion requests resulted in incomplete deletion or mere "de-identification" of user data, with collected data in some cases being retained "indefinitely".

The report also focuses extensively on company practices related to platform usage by children and teenagers—over which FTC Commissioners of both political stripes have expressed concern. The report stated that, in many cases, companies "bury their heads in the sand" to the fact that children use their services. For instance, despite formal company policies that restrict account creation to those over the age of 13, the report found that 40% of children between the ages of 8 and 12 use some form of social media. The report finds that some companies intentionally restrict using data analytics to determine whether users were below the age of 13, despite using that technology to infer the ages of other users.

The report states that companies generally do not offer protections beyond the legal requirements set forth under the Children's Online Privacy Protection of 1998 (COPPA). Consequently, teens (who are not protected under COPPA) are often treated "as if they were traditional adult users" and are generally permitted to create platform accounts without parental consent. Teens generally are not distinguished from adults for the purposes of data collection and processing. The application of algorithms, data analytics and AI to users' and non-users' personal information has been found to be "widespread", and users "lack any meaningful control over how personal information was used for AI-fueled systems". As a result, automated data processing has been found capable of prioritizing "certain forms of harmful content" for children and teens.

Lastly, the report sets forth a summary of FTC staff recommendations to address the issues identified.

To what extent the report reflects the view of the Commission moving forward is unclear. First, it is a staff report. Second, it elicited dissents. Commissioner Ferguson issued a partial dissent. While he voted to approve the publication of the report "because it sheds light on the online privacy crisis" and for its discussion of children and teens, he disagreed with applying existing laws using "novel, dubious theories" and instead supported legislative improvements to be adopted by Congress. In addition, Commissioner Ferguson dissented from the report's findings pertaining to targeted advertising and use of AI, expressing skepticism that content moderation should come through government regulatory action. Commissioner Melissa Holyoak additionally dissented in part from the report, expressing concerns over potential regulatory overreach and that the report's analysis gave insufficient attention to potential impacts on free

speech, competition, and consumer welfare, while also urging Congressional action in addressing the online privacy of children and teens. Ultimately, a change in leadership at the FTC may do little to alter the agency's aggressive enforcement of laws like COPPA under well-established legal theories, but the agency may be less inclined to apply novel theories to expand the scope of regulation under existing legislation.

DEVELOPMENTS IN CHILDREN'S PRIVACY

As is suggested in the FTC staff report, there has been significant federal attention given to children's online privacy safety over the past several years, which is a trend that is likely to continue. Indeed, the release of the FTC staff report came not long after the FTC's December 2023 notice of proposed rulemaking to update the rule promulgated by the FTC pursuant to COPPA, set forth in 16 CFR Part 312 (COPPA Rule). As we've previously discussed[2], the proposed revisions to the COPPA Rule include expanding the definition of covered "personal information" to include biometric data, expanding data security requirements and requiring operators to obtain separate, verifiable parental consent to disclose information to third parties. The revised COPPA Rule's comment period closed on March 11, 2024. It remains to be seen what changes new FTC leadership may bring with respect to the treatment of children's online privacy and how the proposed changes to the COPPA Rule will be affected.

Parallel to the FTC's efforts to bolster the COPPA Rule, members of Congress may reintroduce the "COPPA 2.0" and the Kids Online Safety Act (KOSA) bills. COPPA 2.0 was originally introduced by Sens. Ed Markey (D-Mass.) and Josh Hawley (R-Mo.) in 2019. The COPPA 2.0 bill would extend COPPA's requirements to children up to the age of 16; require online services to implement more stringent data privacy measures for children; mandate greater transparency in how children's data is collected, used and shared; and ban targeted advertising to children. Additionally, the bill would provide parents with more control over their children's online activities and data, including the right to delete collected personal information.

In addition to COPPA 2.0, the KOSA bill, first introduced in 2022 by Sens. Richard Blumenthal (D-Conn.) and Marsha Blackburn (R-Tenn.), was reintroduced in 2023. KOSA would require online platforms to implement various controls for the protection of children, including enabling a platform's strongest privacy settings by default, disabling certain addictive design features and allowing for the restriction of algorithmically recommended content.

Both COPPA 2.0 and KOSA passed in the Senate on July 30, 2024, as the combined "Kids Online Safety and Privacy Act" (S.2073), by a vote of 91-3. A revised version of the Senate bill was sent to the House on September 18, 2024 (H.R.7891), but ultimately was not passed prior to the adjournment of the 118th Congress. It is yet unclear how FTC leadership changes in the wake of the 2024 election and the convening of the 119th Congress will affect future attempts to pass similar legislation.

ENFORCEMENT NEWS

CFPB Guidance on the Use of Third-Party Consumer Reports in Employment Decisions

On October 24, the Consumer Financial Protection Bureau (CFPB) issued guidance advising that companies using third-party consumer reports—including background dossiers and surveillance-based "black box" AI or algorithmic scores about their workers—must follow Fair Credit Reporting Act (FCRA) rules. The guidance states that companies must ensure the accuracy and privacy of the information used

2 For more information, please refer to Cravath's January and July 2024 Privacy and Security Review publications.

in third-party consumer reporting agency reports, provide clear disclosures to employees about the use of such reports, obtain explicit consent from employees before collecting or using their data and offer employees the opportunity to review and dispute any information contained in such reports.

The guidance further states that enforcers of federal consumer financial law should consider two key questions in evaluating whether an employer that makes employment decisions based on a report from a third-party consumer reporting agency is regulated by the FCRA. The first is whether the employer's use of data qualifies as a use for "employment purposes" under the FCRA. And the second is whether the report was obtained from a "consumer reporting agency". The FCRA defines "employment purposes" as using a report to evaluate a consumer for employment, promotion, reassignment or retention. This means the FCRA applies to both initial employment evaluations and ongoing employment decisions. A third party can be considered a "consumer reporting agency" if it collects consumer information to furnish reports to employers, including if it collects consumer data in order to train an algorithm that produces scores or other assessments about workers.

The guidance serves as a reminder of the due care that must be exercised as companies continue to adopt new reporting services and monitoring technologies for the evaluation of current or prospective employees, including assessing whether such evaluation practices might violate FCRA rules.

CFPB Finalizes Data Portability Rule for Customers of Financial Institutions

On November 18, the CFPB finalized a rule granting consumers enhanced rights over their personal financial data. This final rule, implementing Section 1033 of the Consumer Financial Protection Act (CFPA) and coming into effect on January 17, 2025, mandates that financial institutions that constitute "data providers" must, upon request and without charge, allow consumers to access and transfer their financial data to other financial service providers.

"Data providers" are broadly defined to include "depository institutions (including credit unions) and nondepository institutions that issue credit cards, hold transaction accounts, issue devices to access an account, or provide other types of payment facilitation products or services". The scope of financial data subject to the rule is defined as "covered data", which includes "information about transactions, costs, charges, and usage". The rule further stipulates that financial institutions must ensure that covered data can only be used for the purposes requested by the consumer and that third parties cannot use such data for other purposes. The CFPB stated that the adoption of the rule was meant to empower consumers "to access account data controlled by providers of certain consumer financial products or services in a safe, secure, reliable, and competitive manner".

Update: DOJ Rulemaking on "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons"

In July of last year, we discussed the March 2024 issuance by the Department of Justice (DOJ) of an advance notice of proposed rulemaking (ANPRM) in response to President Biden's Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern". The ANPRM initiated the rulemaking process required by the Executive Order, aiming to regulate "data brokerage" (defined as "the sale of, licensing of *access* to, or similar commercial *transactions* involving the transfer of data from any *person* (the provider) to any other *person* (the recipient), where the

recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data") to restrict the sale of U.S. data to entities linked to certain "foreign countries of concern" (namely, China, along with Hong Kong and Macau, Russia, Iran, North Korea, Cuba and Venezuela).

On October 29, the DOJ issued a follow-up notice of proposed rulemaking (NPRM), setting forth a proposed rule and expanding upon and clarifying certain aspects of the ANPRM in response to public comments—for example, clarifying that U.S. subsidiaries of foreign entities qualify as "U.S. persons", adding new categories of exempt transactions and revising the definition of a "covered data transaction" to any transaction that involves any access to the data by the counterparty to a transaction rather than any transaction that involves government-related data or bulk U.S. sensitive personal data. The NPRM comment period terminated on November 29 and the DOJ issued the final rule on December 27. It remains to be seen what impact, if any, that new DOJ leadership will have on the implementation and enforcement of the rule.

Other Actions

- Class Action: *Katz-Lacabe et al. v. Oracle America, Inc.*

  On July 18, Oracle agreed to pay $115 million to settle a class-action lawsuit alleging that the company illegally collected and sold users' personal information, including web browsing histories, in-store purchases and geolocation data. The lawsuit, filed in the U.S. District Court for the Northern District of California, claimed that Oracle tracked users online and offline and sold (or otherwise made available) user personal information to third parties (including marketers) without consent. Pursuant to the terms of the settlement, and without admitting any wrongdoing, Oracle agreed to not capture certain "complained-of electronic communications" and create an audit program to review its customers' compliance with contractual consumer privacy obligations. The settlement, which covers people whose personal information was collected or sold by Oracle since August 19, 2018, was granted final approval by the court on November 15.

- Class Action: *Doe et al. v. GoodRx Holdings, Inc. et al.*

  In July 2023, we referenced the FTC's levy of a $1.5 million civil penalty against GoodRx, a California-based digital health platform, for its breach of the Health Breach Notification Rule stemming from its failure to report its unauthorized disclosure of consumer health data to various third parties. A few days after the FTC settlement was announced, plaintiffs brought an action against GoodRx in the U.S. District Court for the Northern District of California, bringing largely the same allegations set forth in the FTC action. On November 25, the plaintiffs and GoodRx entered into a $25 million settlement, subject to court approval. Codefendants named in the action, including Meta and Google, did not participate in the proposed settlement.

- Class Action: *Stark et al. v. Patreon, Inc.*

  On August 1, Patreon agreed to pay $7.25 million to settle a class-action lawsuit alleging violations of the VPPA. The lawsuit, filed in 2022 in the U.S. District Court for the Northern District of California, claimed that Patreon disclosed subscribers' video viewing information to third parties without consent through the use of tracking pixels. The settlement includes a fund to compensate affected subscribers and measures to enhance Patreon's privacy practices. The court granted preliminary approval of the settlement, and a final fairness hearing is scheduled for early 2025.

- FTC & DOJ: *U.S. v. Verkada Inc.*

  On September 4, the FTC and the DOJ announced a $2.95 million penalty and a permanent injunction against Verkada Inc. to resolve a lawsuit alleging that Verkada failed to implement reasonable security measures for the protection of customer data. These failures allegedly exposed sensitive information—including security-camera footage of consumers visiting locations such as hospitals and schools—to unauthorized access. In addition, Verkada was alleged to have violated the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act by sending prospective customers commercial emails and failing to (1) include the option to unsubscribe or opt out, (2) honor opt-out requests and (3) provide a physical post address in the emails. The settlement requires implementation of a comprehensive compliance program to prevent future violations and mandates regular audits to ensure adherence to privacy standards.

- Class Action: *Lopez et al. v. Apple Inc.*

  On January 2, 2025, Apple agreed to pay $95 million to settle a class-action lawsuit alleging violations of state and federal privacy laws, including the Electronic Communications Privacy Act and the California Invasion of Privacy Act. The lawsuit, which was first filed in August 2019 in the Northern District of California, claimed that Apple recorded conversations of users of its voice-activated Siri software without consent. The proposed settlement, which requires court approval, would cover claims for tens of millions of Apple customers who owned Siri-enabled devices from between September 17, 2014 (the date on which Apple incorporated voice activation functionality in its Siri software) and December 31, 2024.

Federal—Cybersecurity

SECURITIES EXCHANGE COMMISSION (SEC) ACTIONS

SEC Charges Four Companies with Misleading Cyber Disclosures

On October 22, the SEC charged four companies—Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited—with making materially misleading disclosures regarding cybersecurity risks and data breaches that each had suffered. The companies were each found to have downplayed cyber-intrusions stemming from the 2020 SolarWinds Orion hack, ranging from posing intrusions as hypotheticals despite having actual knowledge of breaches to downplaying the impact of disclosed intrusions. Without admitting or denying the SEC's findings, the companies each agreed to cease and desist from future violations and pay civil penalties ranging from $990,000 to $4 million and to settle the SEC's charges.

SEC Commissioners Hester Peirce and Mark Uyeda issued a dissenting joint statement, claiming that the information that was omitted from the companies' disclosures was immaterial and accusing the SEC of playing "Monday morning quarterback" in the wake of an unprecedented cyberattack. Specifically, Commissioners Peirce and Uyeda objected to several of the SEC's claims that certain undisclosed information was material, including failure to identify the SolarWinds hack as attributable to a nation-state threat actor, failure to specifically quantify the number of potentially impacted customers or impacted data and failure to update generic risk factors to identify the SolarWinds breach. In the view of Commissioners Peirce and Uyeda, such disclosure would be unlikely to be material to investors.

SEC v. SolarWinds

As we've previously discussed, on October 30, 2023, the SEC filed a complaint in the U.S. District Court for the Southern District of New York alleging, among other things, that SolarWinds knew of the company's cybersecurity risks and vulnerabilities but misled investors regarding cybersecurity practices, and that the SolarWinds chief information security officer also knew of such risks and vulnerabilities but failed to resolve or sufficiently raise them within the company. On July 18, SolarWinds' motion to dismiss was granted in part and the majority of claims were dismissed, with the exception of claims alleging that the company's website "Security Statement" was materially false.

Notably, the Court dismissed the SEC's (1) internal accounting controls claims, holding "cybersecurity controls are outside the scope of Section 13(b)(2)(B)", and that the "text of the statute strongly supports that the term 'system of internal accounting controls' . . . refers to a company's *financial accounting*"; and (2) disclosure controls and procedures claims, holding SolarWinds had a system of controls for disclosure of cybersecurity risks and incidents and that the SEC had not adequately pled that the disclosure controls and procedures had systemic deficiencies or resulted in a failure to properly disclose prior incidents and vulnerabilities. Coming soon after the June 2024 *R.R. Donnelley* settlement we've previously discussed, this ruling represents a setback for the SEC's ability to exert direct oversight over cybersecurity practices through the internal accounting controls provisions.

ENFORCEMENT NEWS

DOJ's Qui Tam Intervention in Action Against Georgia Institute of Technology (Georgia Tech)

On August 22, the DOJ intervened in a cybersecurity qui tam lawsuit for the first time since launching its Civil Cyber-Fraud Initiative in late 2021. The case, filed by current and former members of Georgia Tech's Cybersecurity team, alleges that Georgia Tech failed to meet cybersecurity standards outlined in the Defense Federal Acquisition Regulation Supplement. The lawsuit was filed under the False Claims Act, which allows private individuals to sue on behalf of the government for false claims and share in any recovery. The DOJ's intervention signals increased scrutiny and enforcement of cybersecurity compliance for government contractors. Contractors found in violation could face significant penalties, including damages and fines.

NOTABLE ACTIONS

HHS OCR: HIPAA Settlements

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules, which set forth the requirements that covered entities (health plans, health care clearinghouses and most health care providers) must follow to protect the privacy and security of protected health information (PHI). H2 2024 has seen a notable uptick in OCR settlements with various medical service providers related to the Privacy and Security Rules; of the 13 settlements and penalties brought by OCR for violations of the Privacy or Security Rules in 2024, all but three have been announced since August 1. Of particular note:

- On December 10, OCR settled with Inmediata Health Group, LLC for $250,000 over potential violations of the HIPAA Security Rule. The settlement addressed the impermissible disclosure of PHI that was made publicly accessible online, affecting over 1.5 million individuals. OCR's investigation revealed multiple security failures, including inadequate risk analysis and system monitoring.

- On December 5, OCR imposed a $548,265 penalty on Children's Hospital Colorado for multiple HIPAA Privacy and Security Rules violations following email phishing and cyberattacks in 2017 and 2020. The breaches compromised the PHI of more than 10,000 individuals, and OCR's investigation found that the hospital failed to implement necessary safeguards and training.
- On December 3, OCR announced a $1.19 million penalty against Gulf Coast Pain Consultants for systemic HIPAA Security Rule violations. The violations were discovered following a breach report filed by Gulf Coast Pain Consultants in 2019 indicating that a former contractor had impermissibly accessed the company's electronic medical record system, affecting approximately 34,310 individuals.
- On October 31, OCR settled a ransomware cybersecurity investigation with Plastic Surgery Associates of South Dakota for $500,000. The investigation, which followed OCR's receipt of a breach report in 2017, revealed multiple security failures, including inadequate risk analysis and management, leading to a breach affecting 10,229 individuals. The settlement includes a corrective action plan and a two-year monitoring period to ensure compliance.

On the heels of this uptick in enforcement actions, on December 27, OCR issued a proposed rule to modify the HIPAA Security Rule to require health plans, health care clearinghouses and most health care providers and their business associates to strengthen cybersecurity protections for individuals' protected health information.

Other Actions[3]

- FTC: Marriott International

  On October 9, Marriott International settled for $52 million with the FTC and the attorneys general of 49 states and the District of Columbia for a series of data breaches that occurred between 2014 and 2020, including in connection with Starwood Hotels & Resorts Worldwide LLC, which Marriott had acquired in 2016. The settlement additionally requires that Marriott "implement a robust information security program" to remedy the deficiencies that exposed the personal data of 344 million customers through a series of three separate breaches.

- Federal Communications Commission (FCC): T-Mobile

  On September 30, the FCC announced a settlement with T-Mobile to resolve investigations into multiple data breaches affecting millions of U.S. consumers in 2021, 2022 and 2023. The settlement requires that T-Mobile address security flaws that enabled the breach, including by adopting zero trust network architecture and adopting phishing-resistant multifactor authentication. As part of the agreement, T-Mobile will invest $15.75 million in cybersecurity enhancements and pay an additional $15.75 million civil penalty. The FCC believes these measures will set a new standard for the mobile telecommunications industry. The FCC described the settlement as part of a "renewed focus" by the FCC's Privacy and Data Protection Task Force to enhance consumer data protection across all major wireless carriers.

3 See also the "Verkada" matter in the "Federal-Privacy Notable Actions" section, above.

- FCC: AT&T

  On September 17, the FCC announced a $13 million settlement with AT&T to resolve an investigation into the company's supply-chain integrity and its failure to protect customer information in connection with a data breach of a vendor's cloud environment. The vendor, used by AT&T to generate and host personalized video content, failed to destroy or return customer information as required by contract, leading to a breach in January 2023. The settlement requires AT&T to enhance its data governance practices, including by tracking customer data, enforcing vendor retention and disposal obligations, implementing multifaceted vendor controls and conducting annual compliance audits.

- SEC: ICBC Financial Services

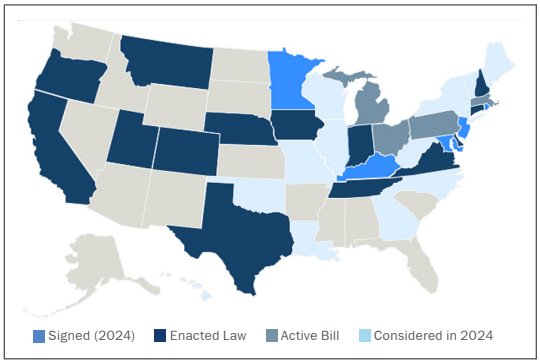
  On December 2, the SEC settled charges against ICBC Financial Services related to a November 2023 ransomware attack without imposing civil penalties because of ICBC's prompt adoption of remedial measures and cooperation with the SEC's investigation. The ransomware attack, which disrupted ICBC's ability to update certain of its books and records, was addressed through "meaningful cooperation" with the SEC and "extensive remedial measures" undertaken by the company.

- SEC: Flagstar

  On December 16, the SEC announced a $3.55 million settlement with Flagstar Financial, Inc. for making materially misleading statements regarding a cybersecurity attack on Flagstar's network in late 2021. Specifically, the SEC found that Flagstar had negligently made materially misleading statements in its public filings regarding the breach, which involved the exfiltration of PII of approximately 1.5 million individuals. In its public filings, Flagstar, among other things, failed to update its risk factors to disclose the breach and, in its disclosure of the breach, failed to state that customer PII was exfiltrated..

State—Privacy

STATE DATA PRIVACY—YEAR IN CONCLUSION



We reported in the first half of 2024 that seven states (Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey and Rhode Island) had enacted comprehensive privacy laws. The second half of 2024 constituted somewhat of a consolidation period in which no new comprehensive bills were passed other than Colorado's Protect Privacy of Biological Data law, expanding the scope of the 2021 Colorado Privacy Act (to protect all biological data that is "generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions, which data is used or intended to be used, singly or in combination with other personal data, for identification purposes"). In addition, on December 21, New York Governor Kathy Hochul signed the "legislative oversight of automated decision-making in government act" (LOADinG Act) into law, which, among other things, restricts the use of AI in certain state government applications and requires human oversight over automated decision-making systems.

The latter half of 2024 has seen a steady stream of adopted legislation beginning to take effect. As we've already discussed, the Oregon Consumer Privacy Act and the Texas Data Privacy and Security Act took effect on July 1 and Montana's Consumer Data Privacy Act followed suit on October 1. In addition, on July 1, certain provisions of various state legislation took effect in Connecticut (pertaining to the right of guardians to delete a minor's social media account), Colorado (pertaining to opt-outs for targeted advertising), and in New Hampshire, Oregon and Tennessee (in each case, July 1 constituted the cut-off date following which data protection assessment requirements apply). Additional obligations took effect in Connecticut on October 1 (pertaining to additional obligations for data controllers with respect to minors).

On January 1, 2025, Delaware's Delaware Personal Data Privacy Act, Iowa's Iowa Consumer Data Protection Act, Nebraska's Nebraska Data Privacy Act and New Hampshire's RSA 507-H all went into effect, along with various provisions of legislation in Colorado, Connecticut, Texas, Montana, New Hampshire and Minnesota. Throughout 2025, adopted legislation will continue to take effect, including New Jersey's Senate Bill 332 (January 15, 2025), Tennessee's Tennessee Information Protection Act (July 1), Minnesota's Minnesota Consumer Data Privacy Act (July 31), and Maryland's Maryland Online Data Privacy Act (October 1), as well as certain provisions of statutes in Colorado, Delaware, Oregon and Indiana.

CALIFORNIA

FCC-CPPA Partnership

On October 29, the FCC announced a new partnership with the California Privacy Protection Agency (CPPA). The partnership seeks to facilitate coordination between the federal and state agencies with respect to privacy, data privacy and cybersecurity enforcement matters, including the sharing of expertise and resources and the coordination of investigations and prosecutions. The announcement marks the FCC's first partnership with a state agency devoted solely to privacy and data protection.

Speaking of the announcement, FCC Enforcement Bureau Chief Loyaan A. Egal said: "Protecting the digital privacy and data of nearly 40 million Americans located in California is vitally important. Together, CPPA and FCC policy makers and enforcers can ensure that federal and state protections are coordinated and maximized for the benefit of everyone across the state."

CCPA Updates

On November 8, the CPPA Board voted to adopt new regulations regarding data broker registration requirements. The new regulations clarify provisions in the Delete Act, which requires data brokers (defined in California Civil Code section 1798.99.80 as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship", subject to limited enumerated exceptions) to register with the CPPA. Specifically, the newly adopted regulations, which took effect on January 1, 2025, clarify various defined terms including "direct relationship", "minor" and "reproductive health care"; require data brokers to disclose certain information regarding their exempt data collection practices; and clarify the procedures for data broker registration.

In addition, the CPPA Board advanced into formal rulemaking a rulemaking package for insurance, cybersecurity audits, risk assessments and automated decision-making technology (ADMT). The formal rulemaking package serves to update existing CCPA regulations, clarify the interplay between insurance laws and the CCPA, require certain businesses to conduct annual cybersecurity audits and risk assessments and establish consumer rights to opt out of businesses' use of ADMT. The written comment period closes on January 14, 2025.

ILLINOIS

On August 2, an amendment to Illinois's Biometric Information Privacy Act (BIPA) was signed into law. The amendment, which went into immediate effect, significantly limits the potential for recoveries for BIPA violations by deeming that multiple disclosures of the same biometric information shall constitute only one violation (rather than separate violations for each disclosure). The amendment comes in the wake of the Illinois Supreme Court's finding in the 2023 case of *Cothron v. White Castle System Inc.*, in which the Court determined that BIPA violations accrue with "every scan or transmission" of biometric information—leading to the potential for astronomical damages where companies use biometric data for routine tasks such as employee timekeeping. The amendment additionally permits consent for the collection of biometric information to be obtained through electronic signatures.

State—Cybersecurity

NEW YORK

On November 1, various requirements of the amended New York Department of Financial Services (NYDFS) cybersecurity regulations for financial services companies took effect. Specifically, "covered entities" (i.e., non-exempt companies regulated by the NYDFS) must now comply with new chief information security officer internal reporting requirements, new cybersecurity oversight responsibilities for company management, expanded data encryption obligations and new requirements pertaining to incident response, continuity and disaster recovery plans. In addition, various other requirements set forth during the regulatory transitional period will take effect in 2025, including expanded recordkeeping practices and audit trails "designed to detect and respond to cybersecurity events", enhanced written policies governing secure development practices for in-house software, information technology asset inventory tracking and implementation of written policies "designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers".

On October 16, NYDFS issued guidance on the cybersecurity risks associated with AI and strategies to mitigate such risks. The guidance outlines specific AI-related threats, such as AI-enabled social engineering (e.g., creation of "deepfakes"), AI-enhanced cyberattacks and vulnerabilities posed to companies by their deployment of nonpublic information to operate AI products or use of third-party vendors that process AI-fed data. The guidance emphasizes the importance of robust risk assessments, access controls, third-party management and cybersecurity training.

On November 25, New York Attorney General Letitia James and DFS Superintendent Adrienne A. Harris announced $11.3 million in penalties against GEICO and Travelers Indemnity Company for inadequate data security that compromised the personal information of over 120,000 people. Hackers reportedly exploited vulnerabilities in the companies' online insurance quoting tools to steal drivers' license numbers and other personal data, which were later used for fraudulent unemployment claims during the COVID-19 pandemic. The investigations revealed that both companies failed to implement sufficient cybersecurity measures as required by NYDFS regulations. As part of the settlements, GEICO will pay $9.75 million and Travelers $1.55 million, and both companies are required to enhance their cybersecurity practices.

PENNSYLVANIA

On September 26, an amendment to the Breach of Personal Information Notification Act (BPINA) went into effect. The amendment includes a new obligation to notify the Pennsylvania attorney general and offer credit reports and monitoring services if a data breach affects more than 500 Pennsylvania residents. The notification must include a summary of the breach, including the estimated number of impacted individuals. In addition, the amendment provides for the creation of a new online portal on the Pennsylvania attorney general's website for the reporting of breaches.

Global

EUROPE

Implementation of NIS2 Directive, the EU's Expanded Cybersecurity Directive

The NIS2 Directive is an EU law on cybersecurity adopted in 2022 that endeavors to set minimum cybersecurity requirements for certain in-scope companies across the European Union, and to update EU cybersecurity rules that were first introduced in 2016. The law included an obligation for EU member states to adopt the NIS2 Directive into their respective national laws by October 17, 2024. Among its requirements, the NIS2 Directive requires in-scope companies to develop risk-management and data security systems, establish cybersecurity incident reporting requirements and assign new responsibilities to company managers with regard to cybersecurity oversight. On November 28, the European Commission opened infringement proceedings against 23 member states for failure to transpose the NIS2 Directive into national law by the October deadline.

EU AI Act Enters Into Force

On August 1, the EU's Artificial Intelligence Act (AI Act) entered into force. The AI Act regulates providers and distributors of AI technology and categorizes such technology into one of four different risk classifications, which determines the regulatory obligations placed upon distributors of such technology. "Minimal risk" systems, which include "most AI systems, such as AI-enabled recommender systems and spam filters", face no obligations under the AI Act. "Specific transparency risk" systems such as chatbots must disclose to users that they are interacting with a machine, and certain AI-generated content, such as deep fakes, must be labeled and generated in a manner that such content is detectable as having been AI-generated or manipulated. "High risk" systems impact safety and fundamental rights, including AI systems used for making employment or loan issuance determinations or to run autonomous robots, and are subject to strict requirements pertaining to data logging, human oversight and robust cybersecurity measures. Lastly, "unacceptable risk" systems—which include AI systems made to "manipulate human behaviour to circumvent users' free will" and include AI-enabled toys that encourage dangerous behavior in minors, AI systems that allow "social scoring" by governments or companies, certain predictive policing applications and certain workplace monitoring systems—are banned (with narrow exceptions).

The majority of the rules promulgated under the AI Act will take effect on August 2, 2026, though rules pertaining to "unacceptable risk" systems and "general-purpose AI models" (which include models that are trained on large data sets and have the capability to perform a wide range of distinct tasks) apply in February and August 2025, respectively. Companies not in compliance with the rules may be fined up to 7% of their global annual turnover for violations involving banned AI applications, up to 3% for violations of other obligations (including those pertaining to general-purpose AI models) and up to 1% for supplying incorrect information or incomplete information to regulatory authorities.

Nuctech Warsaw and Nuctech Netherlands v. Commission

On August 12, the EU Court of Justice ruled that EU subsidiaries can be required to provide access to data and email accounts held by their overseas parent company. The case, *Nuctech Warsaw Company Limited and Nuctech Netherlands v. Commission*, concerned an investigation into foreign manufacturing subsidies conducted by the European Commission at the premises of subsidiaries of Nuctech, a Chinese state-owned company and security and surveillance equipment supplier. In the course of its

investigation, the European Commission sought to obtain access to email mailboxes of various employees to which Nuctech refused access, claiming that the servers containing the mailbox data were all located in China. Nuctech petitioned the lower-tier General Court of the European Union, seeking relief from the European Commission's request. The General Court denied the request, and instead upheld the European Commission's authority to request information from any business operating within the European Union, regardless of ownership. While the decision is non-final, it highlights the expansive cross-border reach that some European courts may seek to assert in certain regulatory matters.

Europe/U.S.: First report under EU-U.S .DPF

On November 4, the European Data Protection Board (EDPB) adopted a report under the EU-U.S. Data Privacy Framework (DPF). The DPF is a data transfer agreement between the European Union and the United States, established in 2022. Earlier frameworks, such as the EU–U.S. Privacy Shield and the International Safe Harbor Privacy Principles, were invalidated by the European Court of Justice due to worries that personal data transferred out of the European Union could be monitored by the U.S. government. In contrast, the DPF was declared "adequate" by the European Commission on July 9, 2023, finding that the United States had ensured an adequate level of protection (i.e., similar to that of the European Union) for personal data transferred from the European Union to U.S. companies.

The EDPB report acknowledged the efforts by U.S. authorities and the European Commission to implement the DPF, noting developments since the European Commission's adequacy decision pertaining to the DPF in July 2023. These efforts included the U.S. Department of Commerce's steps to implement the certification process for U.S. companies and the establishment of a redress mechanism for EU individuals. The EDPB report emphasized the need for U.S. authorities to provide guidance on compliance requirements for DPF-certified companies and to monitor the practical functioning of safeguards introduced by President Biden's Executive Order 14086. Finally, the EDPB recommended that the next review of the EU-U.S. adequacy decision should occur within three years or less.

Notable Actions

- Irish Data Protection Commission (DPC): LinkedIn

  On October 24, 2024, the Irish DPC fined LinkedIn €310 million (approximately $326 million) for violating the EU's General Data Protection Regulation (GDPR). Specifically, the DPC found that LinkedIn used personal data for targeted advertising and behavioral analysis in a manner that did not validly rely (1) "on Article 6(1)(a) GDPR (consent) to process third party data of its members for the purpose of behavioural analysis and targeted advertising on the basis that the consent obtained by LinkedIn was not freely given, sufficiently informed or specific, or unambiguous"; (2) "on Article 6(1)(f) GDPR (legitimate interests) for its processing of first party personal data of its members for behavioural analysis and targeted advertising, or third party data for analytics, as LinkedIn's interests were overridden by the interests and fundamental rights and freedoms of data subjects"; and (3) "on Article 6(1)(b) GDPR (contractual necessity) to process first party data of its members for the purpose of behavioural analysis and targeted advertising."

- Dutch Data Protection Authority (DPA): Uber

  On August 26, the Dutch DPA fined Uber €290 million (approximately $305 million)

  for violating the GDPR by transferring to servers located in the United States sensitive personal data of European taxi drivers, including location data, photos, payment details, identity documents and, in some cases, criminal and medical data of the drivers. The DPA found that, for a period of over two years, Uber transferred this data to Uber's headquarters in the United States without using transfer tools. Consequently, the protection of personal data was insufficient, constituting a "serious violation" of the GDPR. Uber has stated that it will appeal the fine.

AUSTRALIA

On November 29, the Australian parliament adopted the "Privacy and Other Legislation Amendment Bill 2024" to amend the Privacy Act 1988 (Privacy Act). The amendments to the Privacy Act include introducing a statutory tort for serious invasions of privacy, expanding the Office of the Australian Information Commissioner's enforcement and investigation powers, mandating the development of a Children's Online Privacy Code, creating a mechanism for a "white list" of countries for cross-border data transfers and requiring privacy policies to disclose information about substantially automated decisions affecting individuals' rights or interests. The Australian government characterized the passage of the 2024 bill as the first of two "tranches" of legislation necessary to adopt key reforms that the Government agreed or "agreed in principle" to implement, as set forth in the "Privacy Act Review Report" compiled by the Australian Attorney General. The adoption of the legislation constitutes a significant step forward in achieving Australia's "2023-2030 Cyber Security Strategy" report goal of becoming a "world leader in cyber security by 2030".

CHINA

On January 1, 2025, China's Regulations on Network Data Security Management took effect, implementing key provisions of China's Cybersecurity Law, Data Security Law and Personal Information Protection Law. The regulations apply to both domestic and international entities that process data in China. With respect to foreign entities, the regulations govern foreign businesses collecting personal data for the sale of products or services in China or tracking the behavior of persons in China or activities that otherwise pose a threat to national security, public interest or legal rights of Chinese citizens or organizations. The regulations include the requirement that data processors adopt enhanced network data security including via encryption, data backups, access controls and security authentication. The regulations also prescribe data collection additional protections for "important data" (i.e., data "in certain fields, for certain groups, from certain regions or that reaches a certain scale or precision, which, if compromised, could directly threaten national security, economic stability, social order or public health and safety") and streamline certain restrictions on cross-border data transfers.

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
+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 10001-1696
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