STRADLEY RONON

February 6, 2024

Client Alert | Cyber & Privacy

Retrospective: U.S. Cybersecurity and Privacy Developments in 2023

For much of 2023, it seemed like barely a week would pass by without a new data breach or privacy violation finding its way into the headlines, making it clear that the threat actors of the world have not given up. In response, last year saw several significant federal and state regulatory developments in the cyber and privacy landscape. Regulators will remain focused on these issues and how they might be addressed.

Federal Regulatory Developments

U.S. Securities and Exchange Commission

The U.S. Securities and Exchange Commission (SEC) took a number of aggressive regulatory and enforcement positions in 2023. The agency began the year by suing law firm Covington & Burling to obtain the names of almost 300 clients impacted by a 2020 cyberattack attributed to a nation-state actor. A district court ruling in July required Covington to disclose the identities of seven clients whose material nonpublic information was exposed through the hack. One of those clients has anonymously proceeded to contest the disclosure of its identity.

That same month, the SEC finalized new rules for disclosures regarding cybersecurity risk management, strategy, governance and incident response for public companies subject to the reporting requirements of the Securities Exchange Act of 1934. The new rules require companies to disclose material cybersecurity incidents under Item 1.05 on Form 8-K.

The SEC also initiated litigation against SolarWinds Corp. and its chief information security officer (CISO) in October — the SEC's first action against a CISO. The SEC alleges the company and its CISO defrauded investors by overstating the company's cybersecurity practices and understating or failing to disclose known risks in filings made with the commission. The litigation related to these charges is ongoing.

The SEC has not yet finalized its 2022 proposed rulemaking for other securities market participants (such as broker-dealers, clearing agencies, registered investment advisers and investment companies) for cybersecurity risk management, strategy, governance and incident response. The expectation is that the commission will try to finalize the rules this year.

Federal Trade Commission

Early in the year, the Federal Trade Commission (FTC) initiated several litigations related to alleged Children's Online Privacy Protection Act (COPPA) violations, including against Microsoft, educational technology provider Edmodo and Amazon. Microsoft agreed to pay $20 million to settle charges related to its illegal collection and retention of personal information from

children who signed up for its Xbox Live service. Edmodo agreed to a $6 million civil penalty for its collection of personal data from children, the use of that data in advertising and the unlawful outsourcing of COPPA compliance responsibilities to schools. The FTC's litigation against Amazon remains ongoing.

The FTC also began to enforce the Health Breach Notification Rule in 2023 with respect to the unauthorized sharing of health information in violation of an organization's privacy policy. The FTC settled with GoodRx, a telehealth and prescription drug discount provider, on a no-admit/no-deny basis for $1.5 million in February. In May, the FTC settled with another entity, Easy Healthcare Corp., for $100,000.

In June, the FTC reached a settlement with 1Health.io over allegations the company left sensitive generic and health data unsecured, deceived consumers about their ability to get their data deleted and made retroactive changes to the company's privacy policy without adequately notifying and obtaining consent from customers whose data the company had already collected. These acts constituted unfair or deceptive acts or practices in violation of Section 5(a) of the Federal Trade Commission Act. 1Health.io agreed to pay $75,000 and take additional remedial actions to address the violations.

The FTC settled with BetterHelp Inc. in July over allegations that the company revealed consumers' sensitive data to third parties for advertising purposes after promising in its privacy policy to keep such data private. The company also failed to employ reasonable measures to safeguard the health information it collected from consumers, such as failing to train its employees on how to protect the information when using it for advertising; failing to provide consumers with the proper notice as to the collection, use and disclosure of their health information; and failing to limit contractually the manner in which third parties could use consumers' health information. BetterHelp agreed to pay $7.8 million and to take additional remedial actions to address the violations.

At the start of the fourth quarter, the FTC approved an amendment to the Safeguards Rule (16 CFR 314) of the Gramm-Leach-Bliley Act requiring non-banking financial institutions (such as mortgage brokers, motor vehicle dealers and payday lenders) to report certain data breaches and other security events to the agency. The FTC must be alerted as soon as possible — and no later than 30 days after discovery — of a breach involving the information of at least 500 consumers where unencrypted customer information has been acquired without the authorization of the individual to which the information pertains.

After the FTC sought to impose additional privacy requirements against Meta Platforms Inc. (formerly Facebook Inc.) for alleged violations of its prior 2012 and 2020 privacy settlements, the company sued the FTC to contest the constitutionality of the commission's in-house proceedings and sought an injunction against the FTC's reopening of the 2020 order. A district court judge rejected Meta's arguments in November, and Meta has appealed that decision to the U.S. Court of Appeals for the D.C. Circuit.

In December, the FTC proposed changes to the COPPA Rule that would place additional restrictions on the use and disclosure of children's personal information and the ability of companies to monetize children's data. The proposed rule includes: (1) separate opt-in for targeted advertising; (2) prohibition against conditioning a child's participation in an activity on the collection of personal information; (3) additional requirements around the use of information in support of a website's internal operations; (4) limitations on the use of push notifications to encourage children to remain online; (5) codification of the FTC's guidance on education

technology; (6) increased accountability for COPPA safe harbor programs; (7) a requirement for a written children's personal information security program; and (8) a limit on the retention of personal information to the period necessary to fulfill the specific purpose for which it was collected.

The FTC settled with Rite Aid Corp. in December over the company's use of facial recognition technology for surveillance purposes. Rite Aid allegedly deployed A.I.-based facial recognition technology in an effort to identify customers who engaged in shoplifting or other problematic behavior. However, the company failed to implement reasonable measures to prevent harm to consumers who were erroneously accused of wrongdoing because the facial recognition technology falsely flagged them. The FTC's order banned Rite Aid from using the technology for five years and required other programmatic changes to be addressed.

Consumer Financial Protection Bureau

In October, the Consumer Financial Protection Bureau (CFPB) proposed the Personal Financial Data Rights rule. This rule is intended to provide consumers with more control over their financial data and to effectuate sharing of data at a consumer's direction across companies — so-called "open banking." The rule would require banks and other providers to: (1) make personal financial data available at no charge to consumers or their agents through dedicated digital interfaces that are safe, secure and reliable; and (2) recognize a consumer's legal right to grant third parties access to information associated with credit card, checking, prepaid and digital wallet accounts. Companies receiving data under the rule face strict limitations on what they can do with the information. They are not permitted to collect, use or retain data to advance their own commercial interests through actions like targeted or behavioral advertising.

U.S. Department of Health and Human Services

The U.S. Department of Health and Human Services (HHS)'s Office for Civil Rights issued a proposed rulemaking in April intended to strengthen Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule protections by prohibiting the use or disclosure of protected health information to bring criminal, civil and/or administrative proceedings against patients, providers and others involved in the provision of legal reproductive health care, including abortion.

At the beginning of November, the American Hospital Association (AHA) sued HHS over a rule prohibiting the use of certain online tracking technologies that would result in impermissible disclosures of protected health information to tracking technology vendors or other HIPAA rule violations. In its suit, the AHA claimed the HHS rule exceeded the government's statutory and constitutional authority, failed to satisfy the agency rulemaking requirements and harmed the population it purported to protect. The AHA also noted that the government's own health care providers continued to deploy the prohibited technologies on their websites. The litigation remains ongoing.

Also in November, a nonprofit academic hospital in New York settled with HHS over its sharing of protected health information of COVID-19 patients with a national media outfit in 2020. The hospital had disclosed the information of three patients without first obtaining their written authorization. It agreed to pay an $80,000 penalty and to take remedial actions to address the violations.

Executive Office of the President of the United States

President Joe Biden issued an executive order in October intended to address the development of artificial intelligence (AI), also referred to as language models/generative pre-trained transformers. The White House had previously acted in this space in 2022 through the publication of "Blueprint for an AI Bill of Rights" and in a February executive order directing executive agencies to take further steps to combat algorithmic discrimination, among other things.

The October executive order establishes new standards for AI safety and security. It requires certain developers of "any foundation model that poses a serious risk to national security, national economic security or national public health and safety" to notify the U.S. government and to share safety test results and other critical information. It also calls upon the National Institute of Standards and Technology (NIST) to develop standards, tools and tests to help ensure that AI systems are safe, secure and trustworthy.

The order also called for: (1) new standards for biological synthesis screening to protect against the risks of using AI to engineer "dangerous biological materials"; (2) the establishment of "standards and best practices for detecting AI-generated content and authenticating official content"; (3) the establishment of an "advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software"; and (4) additional work by the National Security Council and White House Chief of Staff to guide the U.S. military and intelligence community in their use of AI.

The executive order also calls upon Congress to pass bipartisan data privacy legislation. The House and Senate have previously conferred on such legislation but it has yet to pass. The executive order also directs: (1) the prioritization of "federal support for accelerating the development and use of privacy-preserving techniques"; (2) research and development on technologies to preserve individuals' privacy; (3) strengthening "privacy guidance for federal agencies to account for AI risks"; and (4) the development of "guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques, including those used in AI systems."

The executive order directs agencies to ensure the "collection, use and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks." It also specifies numerous steps to be taken by specific agencies to bolster privacy protections and mitigate privacy risks potentially exacerbated by AI. These include the development of AI standards that may include "best practices regarding data capture, processing, protection, privacy, confidentiality, handling and analysis." The deadlines in the executive order direct executive agencies to perform most of this work during 2024.

Federal Communications Commission

The Federal Communications Commission (FCC) adopted updated data breach notification rules in December for telecommunications carriers and relay service providers. The new regulations would require notice of breaches to be provided to the FCC as well as the U.S. Secret Service and the FBI. Notification would not need to be provided in those instances where the affected entity could reasonably determine that no harm to consumers is likely to occur due to the breach. That same month, the FCC announced that it had signed memoranda of understanding with the attorneys general of Connecticut, Illinois, New York and Pennsylvania to share expertise and resources and coordinate efforts in conducting privacy, data protection and cybersecurity-related investigations to protect consumers.

U.S. Department of Defense

Not content to sit on the sidelines, the U.S. Department of Defense ended 2023 by proposing a new version of its Cybersecurity Maturity Model Certification program (CMMC 2.0). The proposed rule expands on prior 2019 and 2021 proposals and calls for a tiered model of cybersecurity standards (depending on the type and sensitivity of the information), as well as assessment requirements to allow for the verification of cybersecurity standards. These standards and requirements are to be implemented through the department's contracts.

State Regulatory Developments

Data Privacy Laws

Last year began with one state, California, having a comprehensive data privacy regime in place and another state, Nevada, having certain privacy protections in effect. Privacy acts took effect in Colorado, Connecticut, Utah and Virginia during the year. Nine more states have data privacy regimes that will go into effect between July 1, 2024, and January 1, 2026:

State Law	Effective Date
Florida Digital Bill of Rights	July 1, 2024
Oregon Consumer Privacy Act	July 1, 2024
Texas Data Privacy and Security Act	July 1, 2024
Montana Consumer Data Privacy Act	October 1, 2024
Delaware Personal Data Privacy Act	January 1, 2025
Iowa Consumer Data Protection Act	January 1, 2025
New Jersey Data Privacy Act	January 15, 2025
Tennessee Information Protection Act	July 1, 2025
Indiana Consumer Data Protection Act	January 1, 2026

As of publication, at least another nine states have active privacy bills in their legislatures.

New York State Department of Financial Services

The New York State Department of Financial Services updated its cybersecurity regulations on November 1. The revised regulations: (1) strengthen governance requirements; (2) require additional controls to prevent unauthorized access and prevent or mitigate the spread of an attack; (3) impose requirements for more regular risk and vulnerability assessments, as well as more robust incident response, business continuity and disaster recovery planning; (4) contain updated notification requirements (including a requirement to report ransomware payments); and (5) include updated direction for companies to invest in at least annual training and cybersecurity awareness programs. The intent is to build out the robustness of an organization's cybersecurity program and to ensure it has adequate resources.

My Health, My Data Act

In April, Washington state passed a new act that expands privacy protections for personal health data falling outside of HIPAA. The My Health, My Data Act requires consent or necessity for collecting and processing consumer health data. Regulated entities must obtain separate consent or meet the same necessity standard to share the data. The sale of data requires a written and signed authorization from the consumer. The act contains a definition of consumer health data that is significantly broader than what is typically considered health-related data. (For example, "data that identifies a consumer seeking health care services" is covered by the act.)

Non-small-business regulated entities must comply with the act beginning March 31, 2024, and small businesses must comply beginning June 30, 2024. The act provides for a private right of action, which means that plaintiffs will likely begin testing its boundaries soon after it goes into effect.

California Privacy Protection Agency

The California Privacy Rights Act of 2020 established a new state agency, the California Privacy Protection Agency (CPPA), which the state is transitioning much of its administrative apparatus to for consumer privacy issues. The CPPA has not been content to accept the existing regulatory structure and is emerging as an aggressive actor with further ideas for regulation. In November, the CPPA proposed draft regulations that would define new protections against the use of automated decision-making technologies (ADMT), defined as "any system, software or process — including one derived from machine-learning, statistics or other data-processing or artificial intelligence — that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decision-making." The new regulations would apply to situations where AMDT is used for: (1) decisions about employment or compensation; (2) profiling employees, contractors, applicants or students; (3) profiling consumers in publicly accessible places (such as through facial-recognition technology or automated emotion assessment); and (4) profiling consumers for behavioral advertising. Under the draft regulations, businesses are required to provide pre-use notices; allow consumers to opt out, except in certain cases, such as protecting life and safety; and provide information about how the business uses ADMT to make a decision about a consumer.

In December, the CPPA voted to advance a legislative proposal to require browser vendors to include a feature that allows users to exercise their California privacy rights through opt-out preference signals. Currently, only three browsers (Mozilla Firefox, DuckDuckGo and Brave) offer native support for these signals. Given that several states either currently or will soon require businesses to honor browser privacy signals to opt out of the sale of personal data, it is likely that other states will support this effort.

The CPPA suffered a setback in June when it received an unfavorable ruling that it could not enforce regulations it had created until a year after they had been finalized. This ruling delays the enforcement of the CPPA's initial set of rules, covering topics such as privacy notice requirements and responses to consumer opt-out requests, until March 29, 2024.

Looking Forward

Expect this pattern of stimulus and response to continue through 2024, with regulators continuing to expand their authority to address perceived cybersecurity and privacy threats. Perhaps the greatest spur to regulators will be the continued use of AI. Given the privacy concerns raised by many of these technologies, it does not take an oracle to foresee that a great deal of additional regulation will likely be forthcoming as the world adjusts to the use of these tools.

For more information, contact:

Peter Bogdasarian
Partner
202.419.8405
pbogdasarian@stradley.com

Alycia M. Vivona
Partner and Chair, Mergers & Acquisitions
202.419.8424
avivona@stradley.com