Strategic Perspectives

Privacy and Cybersecurity Rulemaking and Enforcement: Preparing for 2023

By Tony Foley

This is the final installment in a series of three Strategic Perspectives in Cybersecurity Policy Report to help subscribers prepare for the impending applicability of new state laws in 2023, as well as to highlight increasing regulatory and enforcement activity at the state and federal levels. This article, from WK Senior Legal Analyst Tony Foley, discusses the developing landscape in administrative regulation and enforcement of privacy and cybersecurity at the federal and state levels. For Part 1 of the series, on the significant changes made by the California Privacy Rights Act, see here. For Part 2, covering the provisions of Virginia's Consumer Data Protection Act, see here.

As Congress continued to consider (but failed to advance) comprehensive federal privacy legislation in the runup to the mid-term elections, regulators at the federal and state levels stepped into the breach (so to speak), ramping up their activities both in proposing regulations to address issues like cyberincident reporting and data security requirements, and in using their enforcement authority to sanction data controllers that failed to properly notify data breaches or to secure the personal information within their control.

In this article, we'll break down the most significant regulatory proposals currently under consideration by the FTC, SEC, and state privacy regulators, as well as high profile enforcement actions undertaken over the past year. In the absence of preemptory federal legislation, federal and state regulators can be expected to continue down this path, and even to increase their activity, in 2023.

Proposed FTC Rules on "Commercial Surveillance and Data Security"

On August 11, the FTC released an advance notice of proposed rulemaking in which it solicited public comments on proposed rules that are designed to regulate how companies collect, aggregate, protect, use, analyze and retain consumer data, and how they transfer, share, sell of otherwise monetize such data in ways that are unfair or deceptive. The ANPR, which was issued pursuant to the FTC Act's Sec. 18 rulemaking authority, notes that traditionally, the FTC has relied on individual enforcement actions to address consumer harms, but is exploring the potential for the promulgation of specific regulatory requirements.

The ANPR presents commenters with more than 90 questions about widespread collection of personal data, the efficacy of "notice-and-comment" requirements to protect consumers, the ways that personal data can be used for discriminatory purposes, and the potential harms of data processing activities to vulnerable populations like minors. In a statement accompanying the ANPR, FTC Chair Lisa Khan noted that, as the country's de facto law enforcer in the privacy realm, the agency must ensure that its policies regarding enforcement and policy keep pace with the market realities inherent in the ever-evolving world of data collection and processing.

"[T]he growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used—means that potentially unlawful practices may be prevalent, with case-by-case enforcement failing to adequately deter lawbreaking or remedy the resulting harms," Commissioner Khan said in her statement. "The fact that current data practices can have such consequential effects heightens both the importance of wielding the full set of tools that Congress has given us, as well as the responsibility we have to do so." She also

noted that, if Congress were to pass strong federal privacy legislation—a hope that she and her fellow Democratic commissioners share—the Commission would take that opportunity to reassess whether continuing its rulemaking efforts represents a sound use of resources.

Republican commissioners, for their part, expressed concerns that the rulemaking should focus more tightly on data abuses rather than presenting a high volume of open-ended questions on topics they say are outside the FTC's authority. "The [ANPR] provides no notice whatsoever of the scope and parameters of what rule or rules might follow, thereby undermining the public input and congressional notification processes," said Commissioner Noah Phillips in his dissenting statement. Fellow GOP Commissioner Christine Wilson added her concerns that the rulemaking process contemplated by the FTC majority would undermine Congress' efforts to advance comprehensive privacy legislation. "The momentum of the [American Data Privacy and Protection Act (ADPPA), the bill currently awaiting a vote on the House floor] plays a significant role in my 'no' vote on the ANPR announced today" she said in her dissenting statement. "I am gravely concerned that opponents of the bill will use the ANPR as an excuse to derail the ADPPA," Commissioner Wilson said.

Since the ANPR was published, the FTC has received a variety of comments from individuals and industry groups providing feedback on the questions posed by the agency, many of which acknowledged the need to take steps to regulate the collection, use and retention of personal data. Other commenters have criticized the effort as overly broad. On November 17, a coalition of 33 attorneys general offered comments on the ANPR, emphasizing that the FTC should prioritize the harms consumers face through the prevalence of commercial surveillance. In addition, the FTC held an online forum on September 8 in which numerous panelists expressed support for the FTC's effort.

Comments on the ANPR were due by November 21, after a one-month extension of the original deadline. Under the FTC's rulemaking procedures, which are subject to additional steps under the Magnuson-Moss Act, the FTC must issue a Notice of Proposed Rulemaking (NPRM) to outlaw specific unfair or deceptive trade practices, hold informational hearings, and issue a final rule that is subject to judicial review. The specter of judicial review is particularly important given the Supreme Court's recent ruling in *West Virginia v. EPA*, in which the High Court openly signaled its hostility to regulatory overreach based on the "major questions" doctrine. Given all of these factors, it is unlikely that any rulemaking will be finalized until at least late next year.

SEC Rulemaking on Cybersecurity Requirements

The SEC released proposed rules on cybersecurity risk management, strategy, governance and incident notification on March 9. Under the rules, regulated companies would be required to make standard disclosures in their periodic reporting to the SEC, including the addition of a new Item 106 to Regulation S-K that would require companies to provide updated disclosures in periodic reports (i.e., Forms 10-Q or 10-K) about previously reported cybersecurity incidents, (including individually immaterial incidents that become material in the aggregate), describe their policies and procedures for the identification and management of cyber risks, and provide disclosure about their boards' oversight of cybersecurity risk. The new rules also would amend Item 407 of Regulation S-K to require disclosure with respect to whether any member of a regulated company's board has expertise in cybersecurity.

The proposed rules would add a new Item 1.05 for Form 8-K that would require companies to disclose information about a material cybersecurity incident within four business days after a company determines that it has experienced such an incident. Specifically, companies would be required to provide information on when the incident occurred and whether it is ongoing, a description of the nature and scope of incident, whether data was stolen, altered, accessed or used for an unauthorized purpose, the effect of the incident on the company's operations, and whether the company has remediated or is in the process of remediating the incident.

In September the SEC's Investor Advisory Committee (IAC) issued recommendations for enhancements to the provisions outlined above, including requiring companies to disclose key factors in determining the materiality of a cybersecurity incident, extending the proposed reporting requirements on cyber risk management and strategy to registration statements in connection with initial offerings under the Securities Act and the Exchange Act, and reconsidering the requirements regarding disclosures of board member expertise, noting that they may result in oversight falling under the purview of relatively few board members with the requisite technical knowledge and experience. The IAC also said that the rules should address delays in the new notification requirements when requested by law enforcement authorities, and urged the SEC to coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) in CISA's rulemaking process to implement the Cyber Incident Reporting

for Critical Infrastructure Act (CIRCIA) signed into law in March (see below).

It should be noted that the SEC issued proposed rules imposing similar requirements to those described above that would apply to registered funds and investment advisers. Although these rules have received less attention, they will enhance fund and adviser reporting requirements, perhaps most notably by imposing an incident reporting requirement within 48 hours of having a reasonable basis to conclude that an incident has occurred.

The comment period for the proposed rules cybersecurity risk management, strategy, governance and incident notification expired in May and the proposed rules are awaiting further action from the SEC. It's anyone's guess when the rules will be finalized, but regulated companies would be well advised to study the proposal and to begin to prepare for the compliance challenges that the new requirements will bring, if implemented, including planning for the relatively short time frames for required incident reporting, reviewing their cybersecurity governance procedures, and determining what "materiality" means for their particular circumstances. Companies also should be prepared to engage securities counsel at the beginning stages of their incident response programs.

CISA's Rulemaking on Implementation of CIRCIA

As briefly noted above, CISA is charged under the provisions of CIRCIA to promulgate regulations to implement the new law, which imposes specific incident reporting requirements applicable to critical infrastructure entities. Among the most significant provisions in CIRCIA is a requirement that critical infrastructure entities must report significant cyberincidents within 72 hours to CISA, and must report any ransomware payments made within 24 hours of making the payment.

CISA published a request for information in the *Federal Register* on September 12 asking for public comments by mid-November on how CISA should implement the requirements, which industries should be considered "critical infrastructure entities" subject to the requirements, what types of cyberincidents should be reported, and the specific information that should be required to be included in reports. In addition, CISA conducted public listening sessions in several cities across the U.S. to gather additional feedback on the issues described above. Finally, CISA has received comments from IT, rural broadband, and banking and financial industry groups on the rules, many of which encouraged CISA to carefully tailor the definitions applicable to covered entities and incidents.

The provisions of CIRCIA require CISA to issue a notice of proposed rulemaking (NPRM) no later than March of 2024 to address these issues, and to issue a final rule within 18 months of the publication of the NPRM. Accordingly, it will be late 2025 before any rules would take effect. On November 15, Rep. Yvette Clarke (D.-N.Y.), one of the authors of CIRCIA, urged Alejandro Mayorkas, Secretary of the Department of Homeland Security (the parent agency of CISA) to expedite the rulemaking process, expressing concerns that any significant delays would hamper harmonization efforts with other rulemaking efforts underway, including those by the FTC and SEC as outlined above.

As the process shakes out, any business that is engaged in a potential critical infrastructure sector should continue to monitor developments at CISA's webpage dedicated to CIRCIA.

CPPA Rulemaking to Implement CPRA Amendments

The California Privacy Rights Act (CPRA), which was approved by California voters in the November 2020 general election and takes effect on January 1, 2023, made significant changes to the California Consumer Privacy Act (CPPA). [For a comprehensive breakdown of the requirements of the CPRA, please consult this Strategic Perspective from Jena Valdetero, Shareholder at Greenberg Traurig LLC.] One of the most important provisions of the CPRA, which actually took effect in December 2020 after the election result was certified, was the creation of the California Privacy Protection Agency (CPPA) as the dedicated regulatory authority responsible for overseeing the implementation and enforcement of the CCPA and the amendments made by the CPRA (although the Attorney General continues to have a role in CCPA enforcement).

In September 2021, the CPPA began the process of promulgating rules to implement the CPRA amendments. Since then, the CPPA has conducted multiple public meetings to solicit public comments on its proposed rules, launching the formal rulemaking process in June and officially releasing its draft rules in July. In a November 3 notice, the CPPA issued proposed modifications to the draft proposal, including changes made to the original proposal based on public comments. [All documentation concerning the rulemaking, including hundreds of written and oral public comments, is available on the CPPA's regulations page.]

The proposed regulations currently under consideration provide a roadmap for businesses concerning CPRA requirements related to data minimization and the use of opt-out signals, restrictions on the use of "dark patterns" (user interfaces that

potentially impair user decision making regarding their privacy preferences), notice and correction requirements, requests to limit businesses' use of sensitive personal information, requirements governing contracts among entities with which a business shares personal information (including service providers, contractors and third parties), targeted advertising requirements, and enforcement mechanisms, among many other provisions. It should be pointed out that the proposed regulations do not address risk assessments required under the CPRA, nor do they provide guidance on automated decision-making technology; these issues are expected to be taken up in a subsequent round of rulemaking.

The CPRA had originally required the CPPA to issue a final version of the rules by July 1, 2022, but obviously, they missed that date. The CPPA must now prepare a final rulemaking package, which will be submitted to the CPPA Board for consideration and approval. After that, the final rules will be submitted to the California Office of Administrative Law (OAL), which has 30 business days to review and approve the final rules. Given this timeline, it appears that the rules are likely to be finalized in January or February 2023. It is still unclear whether the CPPA will provide some sort of grace period regarding the scheduled enforcement date of July 1, 2023, but it would behoove businesses who are preparing their compliance programs to assume that the CPPA will begin enforcing the rules on that date.

Colorado Privacy Act Rulemaking

The Colorado Privacy Act (CPA), which was signed into law in July 2021 by Gov. Jared Polis (D) and takes effect on July 1, 2023, imposes data protection obligations on businesses and confers a variety of rights on consumers with respect to their personal information. Colorado joined California and Virginia (which were later joined by Utah and Connecticut) as states with comprehensive privacy and data protection laws. However, only the California and Colorado laws authorize regulatory rulemaking. The responsibility for promulgating regulations in Colorado is vested in the Attorney General's Office.

On October 10, the AG's office, under the direction of Attorney General Phil Weiser (D), published its draft rules implementing the provisions of the CPA. The rules provide a great deal of detail beyond the relatively high-level parameters of the CPA, including a specific definition of biometric information, directions on responding to consumer access and correction requests, privacy notice provisions, and specific guidance fleshing out requirements regarding loyalty program disclosures and use of universal opt-out mechanisms. They also discuss the concept of "sensitive data inferences," or inferences made by data controllers based on personal data like racial or ethnic origin, religion, or sexual orientation, among other types of sensitive information. The rules provide that such inferences from any individual age 13 and over must be deleted within 12 hours if the controller collects them without consent. The draft rules also discuss data protection assessment requirements, the use of dark patterns, and the right to opt out of profiling activities.

The period for public comments on the draft rules runs from October 10, 2022 through February 1, 2023, through this comment portal. To be considered for any proposed revisions presented at the rulemaking hearing scheduled for February 1, comments must be submitted on or by January 18. If the rulemaking hearing continues beyond February 1, the comment period will be extended until the end of the last day of the hearing. According to Colorado procedural requirements, once the public hearing is concluded, the AG's office has 180 days to file adopted rules for publication in the Colorado Register, with the rules taking effect 20 days after publication or on a date specified in the final rules. If those dates hold, it appears that the rules could take effect in late August 2023, but the AG's office has indicated that it intends to finalize the rules by the CPA's July 1, 2023 effective date. Accordingly, businesses should carefully analyze the provisions of the proposed rules (and offer whatever comments they wish to be considered in February) to be prepared for their compliance obligations next July.

So What's Up With the ADPPA?

Much of the rulemaking activity described above could easily be obviated by the adoption of the ADPPA, which is bipartisan, bicameral legislation that would establish a single privacy regime at the federal level. The legislation, which overwhelmingly passed the House Energy and Commerce Committee on July 20, had the backing of key legislators, including House E&C Chair Frank Pallone (D.-N.J.) and Ranking Member Cathy McMorris Rodgers (R.-Wash.), as well as Senate Commerce Committee Ranking Member Roger Wicker (R.-Miss.), but crucially, was not supported by Senate Commerce Chair Maria Cantwell (D.-Wash.). The bill is still awaiting a vote on the House floor.

The provisions of the ADPPA contained a number of compromises that have torpedoed the chances of earlier attempts at comprehensive privacy legislation, including preemption of many (but not all) state privacy law provisions and a private right of action in circumstances where the FTC or a state attorney general has refused to conduct an investigation into an alleged violation.

In the wake of the 2022 midterm elections, which saw the Democrats maintain a slight majority in the Senate (which could increase based on the results of the December 6 runoff between Sen. Raphael Warnock and GOP Candidate Herschel Walker) and the Republicans regaining control of the House (albeit narrowly), the prospects for the ADPPA are somewhat muddled. There doesn't appear to be any indication that the current Congress will take the bill up in its lame duck session this year, and once the new Congress convenes in January, legislative priorities may shift away from privacy concerns. The proposal (or something similar to it) is likely to be reintroduced in the new session, but it's worth noting that without the support of Sen. Cantwell, who is likely to seek an augmented private right of action provision, the prospects for progress are less than optimal.

Federal and State Enforcement Activity

In the enforcement realm, at the federal level, the FTC and SEC have traditionally relied on their powers to sanction regulated companies based on their contravention of existing requirements regarding data safeguards or unfair or deceptive acts or practices. At the state level, the California AG's office has an example page with redacted summaries of notices of alleged noncompliance with the CCPA, while other state AGs have brought actions alleging violations of existing data breach notification and consumer protection requirements. Below is a brief summary of some of the most significant enforcement actions brought in the last few months.

On the federal front:

- In September, the SEC reached a settlement with Morgan Stanley Smith Barney in which the financial services giant agreed to pay $35 million to settle allegations that it failed to safeguard customer data on decommissioned electronic devices. Specifically, the company sold these devices in online auctions without wiping them of all data first, and lost track of unencrypted hard drives that potentially contained personal identifying information. The SEC charged Morgan Stanley with failing to adopt written policies and procedures that required all decommissioned devices to be treated as high risk, or to follow its own requirements for documenting data destruction (CPR, Sept. 21).

- In October, the FTC issued a proposed order against online alcohol marketplace Drizly based on the company's alleged failure to implement sufficient data security measures, leading to a data breach that exposed the personal data of more than 2.5 million customers. Of particular interest in this settlement was that the FTC required Drizly's CEO, James Rellas, to implement the same security measures within any company that he moves to after leaving Drizly. It's not unprecedented, but it's extremely rare for these types of sanctions to attach to a CEO (CPR, Oct. 25).

- The FTC, in connection with the Justice Department, reached a proposed settlement with Twitter in May in which the social media company agreed to pay $150 million in civil penalties and implement compliance measures to resolve alleged privacy violations, including collecting telephone numbers and e-mail addresses, supposedly for account verification purposes, but using the information to help companies send targeted advertising to its users (CPR, May 26).

- The FTC and DoJ also reached a stipulated settlement with Weight Watchers subsidiary Kurbo, Inc. in March for illegally collecting the personal information of children under age 13 in violation of the Children's Online Privacy Protection Act (COPPA). Under the settlement, Kurbo agreed to pay $1.5 million in penalties, to implement appropriate data collection procedures to ensure parental consent, and to destroy any data illegally collected (CPR, March 4).

Meanwhile, in the states:

- Earlier this month, 40 state attorneys general reached a settlement agreement under which search engine behemoth Google agreed to Pay $391.5 million to settle allegations concerning its location tracking practices, resulting in the largest AG-led consumer privacy settlement ever (CPR, Nov. 14). This settlement came on the heels of a settlement in October with Arizona Attorney General Mark Brnovich (R) in which Google agreed to pay $85 million to settle similar allegations (CPR, Oct. 5).

- Also this month, state attorneys general obtained settlements with Experian and T-Mobile resolving allegations regarding separate data breaches from 2012 and 2015 that compromised the data of millions of consumers nationwide. The companies agreed to pay more than $16 million and to take several remediation steps, including implementing a comprehensive security program and providing free credit monitoring to affected customers (CPR, Nov. 7).

- On October 18, the New York Department of Financial Services (NYDFS) fined licensed health insurer EyeMed Vision Care LLC $4.5 million based on violations of the agency's Cybersecurity Regulation (23 NYCRR Part 500). EyeMed also agreed to conduct a comprehensive cybersecurity assessment

and to develop a detailed action plan to address any shortcomings identified in that assessment (CPR, Oct. 19).

Key Considerations for 2023

Looking at the flurry of proposed regulations, not to mention the marked increase in enforcement activity just in the last few months, it seems quite clear that regulators are more than willing to become increasingly involved in imposing data security and breach notification requirements on regulated companies at a much broader level than previously contemplated, and to hold companies that have been lax in these areas accountable for the consequences suffered by consumers.

While it's true that most of the regulations are months, and in some cases years, away from being finalized, that's no excuse for businesses to sit on their hands. There are many steps they can take right away to be better prepared to ensure compliance when any new rules do come into effect (and to protect themselves against costly enforcement actions). Among the most important steps:

- Strive for increased awareness of cyber risks and expertise in company boardrooms;
- Be prepared to engage in greater cooperation with government entities to improve security posture and cyber resilience, including consulting with these players on the upcoming new reporting requirements;
- Start to fill in any gaps identified in their current cybersecurity programs so that they will be properly configured once any new requirements take effect; and
- Take a hard look at their company policies concerning ransomware payments with an eye towards resolving any potential regulatory requirements, and review cyber insurance policies in light of the increased threat landscape.

The more work companies can do now to bolster their cyber defenses and to establish written, comprehensive procedures regarding cyberincident responses, the easier it will be for them to avoid issues with regulators when they establish ever more complex cybersecurity regulations.