2023 OUTLOOK

The Year Ahead: Key Cybersecurity and Privacy Issues for 2023

Paul, Weiss, Rifkind, Wharton & Garrison LLP

Paul | Weiss

February 2, 2023

The Year Ahead: Key Cybersecurity and Privacy Issues for 2023

As we move into the new year, the pace of activity across federal, state and international authorities around cybersecurity and privacy continues to accelerate. Significant developments in regulation and enforcement have been accompanied by the crystallization of approaches towards emerging technologies and data types. All of these changes occur against the backdrop of an evolving threat environment facing both public and private sectors.

1. Incident Reporting

- **We expect U.S. regulators will refine existing incident reporting obligations and implement new ones.** In 2022, new legislation and regulations showed a heightened focus on incident reporting in the traditionally regulated financial and critical infrastructure sectors, as well as the expansion of these requirements to all public companies. These developments included the February 2022 Proposed SEC Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies, the passage of the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") in March 2022, and the November 2022 proposed updates to NYDFS Part 500 Cybersecurity Regulations.[1]

- As new regulations are drafted and public-comment periods wrap up in 2023, organizations will have to navigate an increasingly complex landscape of reporting obligations that requires them to become familiar with requirements for when an incident must be reported, what information must be included in its disclosures, what risks arise when reporting an incident, and how to participate in voluntary information-sharing to enable more effective cyber defenses without increasing exposure to enforcement.

2. Ransomware and Cyber Incidents

- **We expect the number and complexity of cyberattacks to continue to increase, leading to, among other things, increased cybersecurity collaboration between the public and private sectors.** Recent high-profile cyber incidents highlight the evolving cyber threats facing both the public and private sectors. These threats have included the theft of federal pandemic relief funds by a Chinese-linked hacking group, as well as ransomware attacks on critical infrastructure, including hospitals. Other recent attacks have involved the large-scale collection of personal data from U.S. persons, as well as more complex social engineering attacks targeting government or corporate actors. The continued cyber-enabled theft of intellectual

[1] CIRCIA adopts the 72-hour reporting requirement for specific categories of data incidents already enshrined in state laws, such as the NYDFS Cybersecurity Regulation. The proposed SEC rules would require public companies to report "material" cybersecurity incidents by Form 8-K within 72 hours of discovery. The proposed updates to NYDFS regulations would expand companies' reporting obligations to include cybersecurity events impacting a third-party service provider, as well as ransomware payments, which must be reported within 24 hours.

property and data from sensitive industries, including defense and telecommunications firms, has also raised economic and national security concerns for the federal government. These concerns are a motivating factor behind recent legislation, such as the Protecting American Intellectual Property Act, which imposes economic penalties for companies and individuals involved in the theft of U.S. intellectual property.

- With such cyber incidents on the rise, we expect that the federal government will seek additional collaboration with the private sector in order to manage the broader scope of cyber threats that may impact national security. This collaboration has been demonstrated recently during the Second Counter Ransomware Initiative Summit hosted at the White House in September 2022, and the "whole-of-society" approach to addressing cybersecurity threats will likely remain an area of emphasis for the Department of Justice. Further collaboration is likely to take place through measures such as public-private information-sharing regarding cyber risks, and additional incentives by government agencies for the training of private sector IT specialists.

3. Cryptocurrency and Cybercrime

- **We expect greater scrutiny from both criminal and civil components of the DOJ of the cryptocurrency space next year.** Last year, the DOJ announced its first director of the National Cryptocurrency Enforcement Team, which has focused on combatting the rising use of digital assets in facilitating cybercrimes and money laundering. In September, the DOJ established a Digital Asset Coordinator Network of federal prosecutors who will focus on prosecuting criminal activity in the digital asset and cryptocurrency space. In December, the DOJ charged four individuals with conspiring to provide material support in the form of cryptocurrency to ISIS. Already this year, the DOJ has charged a crypto exchange, Bitzlato, with unlicensed money transmitting, alleging that the exchange allowed criminals to transfer illicit funds in contravention of U.S. anti-money laundering regulations. The FBI commented in connection with the criminal complaint that it was committed to investigating those that attempt to use cryptocurrency to evade law enforcement. This follows on the heels of a DOJ suit seeking to recover $60 million from Larry Harmon, the operator of Helix, an anonymizing "mixing" service that authorities alleged could send virtual currency in a manner that concealed the owner following Harmon's guilty plea in 2021.

- These developments demonstrate a trend of increased investigative and prosecutorial focus on the use of cryptocurrencies in criminal activity in 2023, which could extend to crypto exchanges, mixers, tumblers, and other entities in the crypto space.

4. Congressional Investigations

- **We expect heightened focus on cybersecurity and perceived foreign threats as subjects of congressional investigations.** The new Republican-controlled House of Representatives recently established the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party ("CCP"), which is charged with investigating the CCP's "economic, technological, and security progress and its competition with the United States." Committee chair Mike Gallagher (R-Wis.) has already stated that he expects to seek testimony from "big tech" companies on data security and the CCP's potential access to U.S. person data. Given the rising level of interest around Chinese technology and data and national security, this could prove to be an active area of congressional inquiry.

5. Board Accountability and Expertise

- **We expect proposed SEC Rules and NYDFS regulations, as well as emerging best practices across industries, to incentivize boards to include members with cybersecurity expertise or to have ready access to such expertise.** Boards are under increasingly greater expectations to understand and provide oversight over organizations' cybersecurity programs, including by ensuring that they receive regular updates from an organization's CISO and other management.

- In particular, proposed NYDFS regulations would expand board responsibilities, which already include oversight over the organization's cyber risk management program, to require boards to have "sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management." Additionally, Proposed SEC Rules would require public reporting of board oversight of cyber risks, as well as

proxy disclosure of the board's cybersecurity expertise. Boards of directors will need to be aware of these obligations and to stay informed as to what constitutes appropriate management of cyber risk sufficient to satisfy their fiduciary and oversight roles, particularly as these evolve in the year ahead.

6. Federal Agency Rulemaking and Enforcement

- **We expect that with heightened regulatory scrutiny of "commercial surveillance" and data collection, including ongoing rulemaking initiatives, companies will need to consider whether to implement more stringent practices for handling consumers' personal data, and particularly information linked to young persons or vulnerable populations.** For example, as regulatory expectations continue to evolve, companies may wish to reevaluate the ways in which they meaningfully inform customers about the company's use of data and data security risks, provide customers the opportunity to opt out of certain data practices, obtain verifiable consent to personal data collection, minimize the amount of data collected and retained, ensure strong encryption and access controls, and/or implement processes for data deletion.

- Rulemaking: The FTC's August 2022 advance notice of proposed rulemaking ("ANPR") on "commercial surveillance" and data security practices reflects the regulator's effort to compel and complement the proposed American Data Privacy and Protection Act ("ADPPA"). Following an extended public comment period on the ANPR, the FTC is now analyzing the proposed rulemaking, with a focus on understanding the most prevalent types of "commercial surveillance," evaluating actual and potential harms, and identifying areas the FTC has not addressed through enforcement actions. Although neither is likely to take effect in 2023, the potential FTC rule and bipartisan ADPPA together represent the federal government's most comprehensive and intense attention to data privacy to date, highlighting its heightened focus on these issues.

- Enforcement: The FTC called its recent settlement with Epic Games its "largest administrative order in history" and the largest penalty ever obtained for an FTC rule violation, and signaled that protecting the public from online privacy invasions and "dark patterns" is a "top priority" for the agency and one that it will continue to pursue through enforcement actions under existing rules. Meanwhile, the CFPB is expected to report on the findings of its inquiry into six "big tech" companies regarding their payment services, including whether and how they engage in "data harvesting" and "data monetization" with respect to customer financial data. The CFPB may be building up to announcing—through guidance and enforcement actions—new consumer financial privacy restrictions based on its UDAAP (unfair, deceptive, abusive acts and practices) authority that purport to place substantive limits on how financial services providers obtain, use, and retain consumer data.

7. ICTS Rulemaking

- **We expect the U.S. Department of Commerce to finalize its latest ICTS rulemaking.** In 2019, then-President Trump signed Executive Order 13873, empowering the Commerce Department to address risks related to foreign adversaries exploiting vulnerabilities in information and technology systems. In January 2021, Commerce issued an Interim Final Rule on Securing the Information and Communications Technology and Services ("ICTS") Supply Chain, implementing that Executive Order (the "ICTS Rule").

- The ICTS Rule created a framework for Commerce to review and prohibit transactions involving ICTS that have been "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries [most notably, China and Russia]" and that pose an "undue or unacceptable risk" to the national security of the United States. In November 2021, Commerce issued a Notice of Proposed Rulemaking to expand the definition of "ICTS" and "ICTS Transaction" to include "connected software applications," which are broadly defined as "software" with "the ability to collect, process, or transmit data via the internet." A final rule appears to be under review by the White House's Office of Information and Regulatory Affairs as of December 2022. Additionally, after Commerce announced two years ago the issuance of subpoenas under the ICTS Rule to multiple Chinese companies, the industry is waiting for an indication as to how Commerce plans to follow up on these inquiries.

8. California, Colorado, Virginia, Utah and Connecticut Privacy Laws Changing or Coming into Effect

- **We expect 2023 will see new or more robust data privacy laws go into effect in California, Colorado, Virginia, Utah and Connecticut affecting businesses serving consumers located in those states.** The new legislation in these states will largely be similar to one another in their broad protection of sensitive data, although there are also some key differences of which businesses will need to be aware. The laws protect consumers of the states in which they are enacted, and therefore, any entity conducting business in and who controls or processes the data of a substantial number of consumers within the relevant states will have to consider the various obligations it might be subject to. These new laws are generally influenced by, and use language adapted from, the European Union's General Data Protection Regulation. Accordingly, the new laws will reflect an approach to data privacy that is quite similar to the EU's approach. Generally, consumers in relevant states will have more control over their data, including rights to access or create copies of personal data, and to opt-out of their data being used for targeted advertising or otherwise sold. Most of the proposed changes will also allow consumers to correct or update their personal data.

9. U.S. - EU Data Transfers

- **We expect 2023 will spotlight the frameworks governing cross-border data transfers between the United States and Europe.** Last year, the European Commission and the United States announced an "agreement in principle" on the new Trans-Atlantic Data Privacy Framework ("TADPF"), which is designed to restore the legal basis for transatlantic data flows, and to address the concerns raised by the European Court of Justice in the July 2022 *Schrems II* decision, by including substantive limitations on U.S. national security authorities' access to data (necessity and proportionality) and the establishment of a new redress mechanism. President Biden also issued the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, which set out the steps the United States will take to implement the framework.

- Companies using standard contractual clauses and binding corporate rules to transfer EU personal data to the United States will see greater legal certainty as the framework and Executive Order are implemented. TADPF is likely to be considered by the European Court of Justice in the not-too-distant future.

- The European Commission also proposed new rules in May 2022 to combat the spread of child sexual abuse material ("CSAM") online. If implemented, legislation would require technology companies to report such material to authorities and would create a new European entity similar to the United States' National Center for Missing and Exploited Children. However, any disclosure rules could run afoul of U.S. federal law prohibiting technology companies from disclosing user data absent certain exceptions, presenting companies with potentially conflicting obligations to navigate.

10. Enactment of AI Regulations

- **We expect that artificial Intelligence ("AI") and other automated decision-making systems will advance in 2023, and we expect there will be a corresponding government focus on the potential cybersecurity and data privacy risks these technologies may present.** The FTC recently announced a focus in upcoming rulemaking on the potential harms from automated decision-making systems, with particular emphasis on algorithmic bias and other impacts on vulnerable populations, for example.

- There has been an increased governmental focus on AI across the United States and Europe in recent years. The United States' National AI Initiative Act came into effect in 2021, providing for a coordinated program across the Federal government to accelerate AI research and develop guidelines for the use of trustworthy AI in the public and private sectors. Proposed laws in the EU have recently gained momentum as well, with the Council of the EU adopting a general approach through the proposed AI Act, which would build off the European Commission's 2021 Proposal for AI Regulation and the Coordinated Plan on AI. These proposals set out frameworks for the development and use of AI-driven products, services and systems, as well as specific definitions for what types of systems would be covered and what types of risks will determine what requirements apply to a given technology. These requirements would be similar to those reflected in U.S. state privacy laws, including in California, Colorado, and Connecticut, which require companies offer consumers the option to opt-out of the use of data in automated decision-making systems.

11. Civil Liability from Biometrics and AdTech Tracking

- Biometric Data: Biometric data, which includes fingerprints, voiceprints, facial or retinal measurements, and other metrics, has become the subject of state regulation and lawsuits in recent years and the rising use of biometrics will likely lead to a corresponding increase in civil litigation related to such data.

- The increasing use of biometric data makes lawsuits more likely to arise under applicable state laws, such as Illinois' Biometric Information Privacy Act ("BIPA") and Texas' Capture or Use of Biometric Identifier Act ("CUBI"). Other states, including Washington, Utah, Virginia, Maryland, and New York, have also passed laws imposing narrower limitations on the use of facial recognition or other specific categories of biometric information.

- BIPA—under which over 100 federal suits have already been brought—authorizes a private right of action for claims involving the collection or use of biometric data without consent, and there has also been an uptick in class action suits focusing on violations stemming from the use of voice recognition technology. 2022 also saw the first litigation under Texas' CUBI as Texas AG Ken Paxton brought suits against Google and Meta for the capture and alleged use of biometric data without obtaining informed user consent.

- Although biometric data has yet to be specifically regulated at the federal level, federal regulators have indicated their attention to these issues. The FTC, for example, has confirmed it is evaluating potential harms from the collection and processing of biometric information for the purpose of upcoming rulemaking.

- Advertising Tracking and Analytics: Recent suits in the United States and Europe have centered around the use of web tracking technologies offered by companies like Google and Meta to deliver and measure the effectiveness of digital advertising. As companies using digital advertising continue to use these online tracking and analytics technologies, civil claims challenging the use of these technologies under privacy laws and other statutory and common law regimes will continue to proliferate in 2023.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Yahonnes Cleary
+1-212-373-3462
ycleary@paulweiss.com

Roberto J. Gonzalez
+1-202-550-4105
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Neil Chitrao, Jessica Finberg, Megan L. Gao, Jordan E. Orosz, Cole A. Rabinowitz and Rosie Vail contributed to this Client Memorandum.