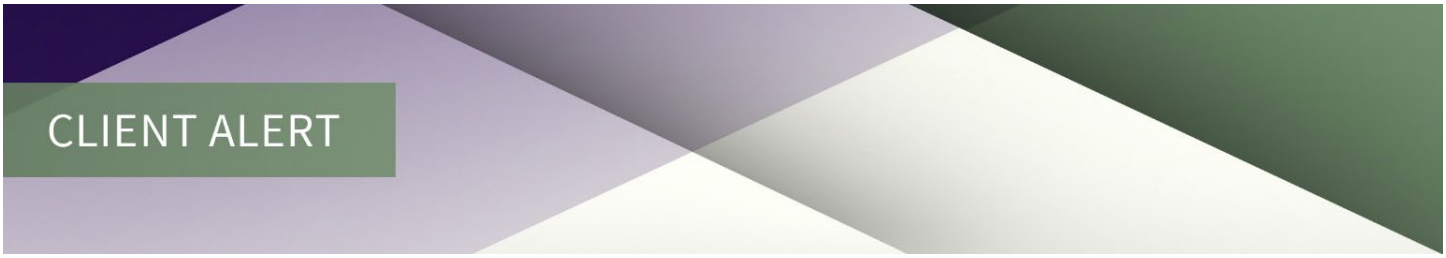

The Year in Privacy, Data Protection, and Cybersecurity: A Timeline of 2022

December 29, 2022

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Kari Prochaska

Uncertainty continued to be the watchword for the privacy, data protection, and cybersecurity legal and regulatory landscape in 2022 – as it has been for some time – though the pace of change seemed to accelerate and the sources of uncertainty seemed to multiply. In the United States, the greatest source of uncertainty was an unlikely one: the Supreme Court. In *Dobbs v. Jackson Women's Health Organization*, the Court upended decades of precedent and common understandings of the constitutional right to privacy, and in the process creating significant concern about how information collected via apps and other digital tools might be used to prosecute doctors and women. Other sources of uncertainty were more predictable, as regulators and legislators at both the federal and state level have continued to move forward with efforts to curb what the U.S. Federal Trade Commission ("FTC") Chair Lina Khan described as an "explosion in data collection and retention [that] has heightened the risks and costs of breaches." While Congress did not succeed in enacting a federal privacy law, thanks in part to heated opposition from California lawmakers, numerous agencies – including the FTC, the U.S. Securities & Exchange Commission ("SEC"), and the Consumer Financial Protection Bureau ("CFPB") – initiated rulemakings proposing to move forward on these topics pursuant to existing statutory authorities. At the state level, several states enacted new comprehensive state privacy legislation, and others enacted issue-specific laws focused on topics including children's and employees' privacy, while state regulators in California, Colorado, and elsewhere took critical steps toward implementing their own privacy laws.

On the cybersecurity front, Russia's invasion of Ukraine in early 2022 sharpened the focus of many in both the public and private sectors on the importance of robust cybersecurity strategies and tactics. While concerns raised by government officials of a possible impending "cyber war" have thus far failed to materialize, the federal government continues to move forward with policies and rules designed to encourage continued vigilance and information sharing. For example, the

Cyber Incident Reporting for Critical Infrastructure Act of 2022 was intended to help facilitate sharing of key information with the Department of Homeland Security ("DHS"), through the Cybersecurity and Infrastructure Security Agency ("CISA"). Meanwhile, the SEC proposed rules to force both public companies and certain registered financial institutions, such as investment advisers and broker-dealers, to take specific steps to improve their own cybersecurity and related disclosures. And the Biden administration continued to move forward with implementing the President's Cybersecurity Executive Order.

Outside the United States, privacy and cybersecurity laws continued to evolve. In Europe, regulators at both the Member State and European Union ("EU") levels continued to grapple with the fallout from Schrems II, pushing companies to do more to keep personal data in Europe. The announcement of a new Trans-Atlantic Data Privacy Framework between the U.S. and EU offered some hope, at least among optimists, that a workable compromise between European privacy concerns and U.S. national security interests had been achieved, allowing personal data to flow freely across the Atlantic. The ongoing maneuvering over cross-border data transfer issues did not stop regulators around the world from ramping up enforcement – most notably, regulators in Ireland issued over $600 million in fines against Meta Platforms for several different alleged violations of the General Data Protection Regulation ("GDPR"). Meanwhile, in Argentina the national data protection regulator proposed new legislation designed to bring Argentina's laws more in line with the GDPR to facilitate an adequacy decision finding. This year also saw Australia become the target of massive ransomware attacks, so much so that the Australian Parliament introduced and quickly enacted legislation that would significantly increase penalties for data breaches to a minimum of AU $50 million.

Below, we offer a timeline of some of the key events, milestones, and actions that defined privacy, data protection, and cybersecurity over the course of 2022. This list is not intended to be comprehensive, but instead seeks to highlight some of the key themes, issues, and questions that arose in 2022 and likely will continue to present challenges in 2023.

Notable Privacy and Cybersecurity Developments of 2022

January

January 1: California SB 41, the Genetic Information Privacy Act, took effect. The Act requires direct-to-consumer genetic testing entities to receive consent from individuals with respect to the collection, use, and disclosure of their personal information, and provides rights of access and deletion. The Act also requires in-scope companies to, among other things, implement reasonable security practices to protect against the unauthorized access, use, modification, or disclosure of genetic data. The California Attorney General may enforce the law, with fines up to $1,000 per incident for negligence and up to $10,000 for intentional violations.

January 4: The FTC asserted its authority over cybersecurity and broader data security matters, warning companies that failure to identify and patch instances of the Log4j vulnerability may violate the FTC Act, stating that the FTC may use "its

full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j or similar vulnerabilities in the future."

January 19: President Biden signed a National Security Memorandum ("NSM") that requires national security systems to deploy the same network cybersecurity measures as required in President Biden's Executive Order 14028 ("EO 14028"), Improving the Nation's Cybersecurity. The NSM establishes timelines and guidance for implementation of cybersecurity requirements under EO 14028; improves the visibility of cybersecurity incidents that occur on national security systems; requires agencies to secure cross-domain tools that transfer data between classified and unclassified systems; and requires agencies to act to protect or mitigate cyber threats to national security systems.

February

February 3: The Department of Homeland Security announced the establishment of the Cyber Safety Review Board ("CSRB"), as directed in EO 14028, on Improving the Nation's Cybersecurity. The CSRB is a public-private initiative that brings together government and industry leaders to elevate national security. According to a DHS press release, the CSRB will review and assess significant cybersecurity events so that government, industry, and the broader security community can better protect the country's infrastructure and networks. The first review was focused on Log4j software vulnerabilities, with a report released in July 2022 highlighting a number of recommendations for organizations to manage both the immediate risks presented by the Log4j vulnerability and longer-term risks related to software supply chain issues.

February 9: The SEC proposed rules related to cybersecurity risk management for registered investment advisers, investment companies and business development companies, as well as amendments to certain rules that govern investment adviser and fund disclosures. Among other things, the proposed rules would require advisers and funds to adopt and implement written cybersecurity policies and procedures; report significant cybersecurity incidents to the SEC and publicly disclose significant cybersecurity incidents that have occurred over the last two years in registration statements; and create new recordkeeping obligations to protect the availability of cybersecurity-related information. (As of December 2022, the proposed rules had yet to be adopted.)

February 24: Utah SB 227, the Utah Consumer Privacy Act, passed the Utah Senate. It passed the Utah House of Representatives on March 3, 2022, and was signed into law by Utah Governor Spencer Cox on March 24, 2022. The law will take effect on December 31, 2023.

March

March 9: The SEC proposed rules to enhance and standardize disclosures regarding cybersecurity risk management strategy, governance, and incident reporting by public companies. Among other things, the proposed rules would require reporting of "material cybersecurity incidents" to the SEC within four days, as well as significant new annual disclosure

requirements related to the company's cybersecurity risk management efforts, including information about any board members with cybersecurity expertise or experience. As of December 2022, the proposed new rules have not been adopted.

March 15: President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), which creates new obligations for owners and operators of critical infrastructure, including an obligation to report certain cyber incidents to the CISA within 72 hours and an obligation to report ransomware payments within 24 hours. The reporting obligations will take effect when CISA promulgates implementing regulations. As of December 2022, CISA has initiated, but not yet completed, its rulemaking.

March 25: President Biden and the President of the European Commission announced that the U.S. and the EU had reached agreement in principle regarding the Trans-Atlantic Data Privacy Framework. U.S. Secretary of Commerce Gina Raimondo and EU Commissioner Didier Reynders announced that they would intensify negotiations to memorialize the Framework in appropriate legal documents. In December 2022, the European Commission released a draft Adequacy Decision on the Framework which must go through an extensive adoption process which incorporates the opinions of other EU regulatory authorities. This process is estimated to take approximately six months.

April

April 13: The California Privacy Protection Agency ("CPPA") announced its plan to hold stakeholder sessions with respect to the rulemaking related to the California Privacy Rights Act of 2020 ("CPRA"). These stakeholder sessions took place May 4-6, 2022; the CPPA would finally commence the formal rulemaking process in July 2022 (see below).

April 19: New Jersey's A.B. 3950, prohibiting certain employer use of tracking devices, took effect. Unlike the comprehensive, omnibus privacy legislation that we have seen in a number of states, this law is an example of state efforts to fill targeted gaps in privacy/data protection absent comprehensive federal privacy legislation, and requires employers to provide notice to any employee who is tracked through a vehicle.

April 28: India's data protection regulator issued guidance relating to "information security practices, procedure, prevention, response and reporting of cyber incidents." In particular, the guidance requires parties to report cyber incidents to India's Computer Emergency Response Team ("CERT-In") within six hours of noticing such incidents or being notified about such incidents.

May

May 3: The European Parliament adopted the final recommendations of the Special Committee on Artificial Intelligence in the Digital Age. These recommendations are intended to inform parliamentary work both at the EU and Member State level, as part of the Commission's Horizon Europe and Digital Europe programs.

May 7: New York's Senate Bill S2628, requiring prior written notice to employees of electronic monitoring, took effect. As with New Jersey's A.B. 3950, this legislation highlights the growing role of targeted privacy/data protection laws at the state level.

May 9: The American Civil Liberties Union announced a settlement of its biometric privacy litigation with Clearview AI. According to the ACLU's announcement, the settlement bans Clearview AI from selling access to its facial recognition database "across the United States."

May 12: The U.S. Department of Justice Civil Rights Division, together with the Equal Employment Opportunity Commission released guidance titled "Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring," explaining how the use of certain technologies in hiring decisions may violate the Americans with Disabilities Act.

June

June 21: H.R. 8152 – the American Data Privacy and Protection Act ("ADPPA") was introduced in the U.S. House of Representatives. The ADPPA was the result of extensive bicameral and bipartisan negotiations, and would have resulted in a broad private right-of-action (a priority for Democrats) with extensive, but not total, preemption of state privacy efforts (a Republican priority).

June 24: The U.S. Supreme Court announced its decision in *Dobbs v. Jackson Women's Health Organization*. The decision, which expressly overturned *Roe v. Wade* and *Casey v. Planned Parenthood*, has profound implications for the constitutional right to privacy, as well as significant practical implications for women's privacy with respect to reproductive health care. In response, the Biden administration engaged in a whole-of-government effort to maximize protection of any information that companies and healthcare providers collect related to women's reproductive health.

June 29: The U.S. Department of Health and Human Services, Office for Civil Rights, released guidance regarding patient privacy protections in the wake of the Supreme Court's *Dobbs* decision, including how patient medical information should be safeguarded when using mobile phones and certain apps.

July

July 8: The CPPA initiated the formal rulemaking process to implement the California Privacy Rights Act by issuing proposed amendments to conform existing regulations under the California Consumer Privacy Act ("CCPA") to the new requirements of the CPRA. The CPPA requested written comments on the proposed regulations by August 23, 2022. The CPPA would release revised proposed amendments in November 2022 (see below); as of December 2022, the amendments had not yet been formally adopted.

July 11: Consistent with the Biden Administration's efforts to protect women's access to reproductive healthcare in the wake of the Supreme Court's *Dobbs* decision, the FTC issued a blog post affirming the agency's commitment to fully enforcing the law against illegal use and sharing of highly sensitive location and health data.

July 29: The New York Department of Financial Services ("NYDFS") proposed amendments to 23 NYCRR Part 500, its Cybersecurity Regulation. Among other things, the proposed amendments would add a new 24-hour notice requirement for any cybersecurity event where an extortion payment has been made, heighten oversight responsibilities of the board of directors and senior management, and create additional cybersecurity requirements for large covered entities by establishing a new class of covered entities called "Class A companies." NYDFS is expected to formally adopt the regulations in the first quarter of 2023.

August

August 11: The FTC initiated a long-awaited rulemaking on commercial surveillance and data security issues by adopting an Advance Notice of Proposed Rulemaking. The FTC cited numerous harms to consumers presented by surveillance issues, and sought comment on the prevalence of these practices and harms, its ability to address them absent some specific rules, and what kind of rules might help to address these harms. The FTC issued this Advance Notice pursuant to its Magnusson-Moss rulemaking authority, which includes a number of procedural steps that the FTC must undertake before it can come to final rules.

August 29: The FTC announced a lawsuit against Kochava Inc. for the sale of sensitive geolocation personal information. According to the FTC, "Kochava's data can reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities," and "Kochava is enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence" without the knowledge or consent of the people to whom the data relates.

September

September 5: The Irish Data Protection Commissioner imposed a €405 million fine, one of the largest GDPR fines to date, against Meta Platforms Ireland Ltd. ("Meta"), alleging violations of the GDPR rules on the processing of children's personal data on Instagram.

September 12: Argentina's Data Protection Authority published a draft bill that would update Argentina's data protection law and bring it more in line with the European Union's GDPR. Among other things, the bill requires data controllers to document and notify the Agency of data breaches within 48 hours of becoming aware of a breach.

September 12: Consistent with its obligations under CIRCIA (see above), CISA issued a Request for Information seeking public comment on the implementation of cyber incident reporting requirements. Numerous stakeholders filed comments,

largely focusing on issues such as the proper threshold for reporting to CISA, what would need to be included in any report, and how quickly such reports must be filed.

September 15: California Governor Gavin Newsom signed AB 2273 – the California Age Appropriate Design Code Act. Among other things, the Act requires certain websites to establish default privacy protections for children's data, and establishes a Children's Data Protection Working Group that is required to report best practices for implementation of the Act to the California legislature by January 2024. The Act will take effect on July 1, 2024.

September 30: Colorado Attorney General Phil Weiser published draft rules implementing the Colorado Privacy Act. Interested parties may submit written comments until February 1, 2023. The announcement also highlighted three public meetings, which took place in November 2022, to discuss the proposed draft rules.

October

October 7: As part of fulfilling the United States' obligations under the Trans-Atlantic Data Privacy Framework, President Biden signed an Executive Order on Enhancing Safeguards for U.S. Signals Intelligence Activities. Within 60 days of the Executive Order, the Attorney General was directed to establish a process for handling complaints under the Executive Order. The European Commission announced that in response to the Executive Order, it would prepare a draft adequacy decision for the United States.

October 24: The FTC issued a proposed order against both Drizly, LLC and its CEO for violations of Section 5 of the FTC Act in connection with Drizly's cybersecurity practices. The FTC's imposition of penalties on the CEO in his personal capacity has significant implications for executives at companies large and small, whose decisions to invest in and prioritize (or not) data security will now be subject to second guessing by regulators and carry the risk of personal liability.

October 27: The CFPB announced a rulemaking to give consumers greater control over their financial data. In particular, the CFPB's proposed rule would establish portability requirements for consumer data collected by financial firms. According to the CFPB, under its proposed rules "consumers would be able to more easily and safely walk away from companies offering bad products and poor service and move towards companies competing for their business with alternate or innovative products and services."

November

November 3: The CPPA released a revised version of proposed amendments implementing the CPRA changes to the CCPA and requested comments on the revised versions of the proposed amendments. Among other things, the revised amendments included language suggesting that the CPPA would take into consideration questions related to the timing of the amendments' adoption in making decisions about enforcement – a concession to commenters who highlighted the practical issues of compliance given the January 1, 2023 effective date of the CPRA's changes to CCPA.

November 9: NYDFS released a second round of amendments to the Cybersecurity Regulation. Among other things, the revised proposed amendments would require that where a covered entity is affected by and aware of a cybersecurity event on the systems of a third-party service provider, notification to NYDFS must be provided within 72 hours. Public comment on the revised proposed amendments is due to NYDFS by January 9, 2023.

November 15: The FTC announced a six-month extension of the deadline for compliance with its updated Safeguards Rule. The update imposed a number of new requirements for covered financial institutions, including designating a qualified individual to oversee their information security program; developing a written risk assessment; limiting and monitoring who can access sensitive customer information; encrypting all sensitive information; training security personnel; developing an incident response plan; periodically assessing the security practices of service providers; and implementing multi-factor authentication for individuals who access customer information. Companies now have until June 9, 2023 to come into compliance.

November 25: The Irish Data Protection Commissioner issued another significant fine to Meta, this time €265 million for violations of GDPR arising from a data leak that resulted in the personal data of approximately 533 million Facebook users worldwide being made available on the Internet.

November 28: Australia's parliament passed amendments to existing Australian privacy law to increase the maximum penalties for serious or repeated privacy breaches from the prior AU $2.22 million penalty to whichever is the greater of (i) AU $50 million; (ii) three times the value of any benefit obtained through the misuse of information; or (iii) thirty percent of a company's adjusted turnover in the relevant period.

December

December 13: The European Commission released a draft adequacy decision that would, if formally adopted, make the Trans-Atlantic Data Privacy Framework ("Framework") a legitimate mechanism for companies transferring personal data from the EU to the U.S. The draft adequacy decision follows President Biden's Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, which endeavors to address European concerns about U.S. government access to personal data of EU data subjects. Among other things, companies seeking to use the new Framework must commit to complying with a detailed set of privacy obligations, including, for example, deleting personal data when it is no longer necessary for the purpose for which it was collected.

December 16: The CPPA Board held a public meeting regarding the status of the CPRA rulemaking process. Among other things, the CPPA announced that the earliest the proposed amendments to the CCPA regulations would likely come into effect would be April 2023, and that it had established a subcommittee to consider regulations regarding risk assessments, cybersecurity audits and automated decision-making, including profiling – the next step in completing the rulemaking directives set forth in the CPRA.

December 19: The FTC announced a "record-breaking settlement with Fortnite owner Epic Games" - $275 million - for alleged violations of the Children's Online Privacy Protection Act ("COPPA"), as well as a second significant settlement - $245 million – related to allegations that Epic was using so-called "dark patterns" that "dupe[d] millions of Fortnite players into making unintentional purchases." The FTC's action highlighted two priorities of Chair Lina Khan: children's privacy and the use of dark patterns.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura Jehl
202 303 1056
ljehl@willkie.com

Kari Prochaska
312 728 9080
kprochaska@willkie.com