Holland & Knight

Data Privacy and Security Report: June 2023

A monthly roundup of federal data privacy and security policy and regulatory news

Welcome back to Holland & Knight's monthly data privacy and security news update that includes the latest in policy, regulatory updates, and other significant developments. If you see anything in this report that you would like additional information on, please reach out to authors or members of Holland & Knight's Data Strategy, Security & Privacy Team.

LEGISLATIVE UPDATES

State Privacy Laws Take Effect; Impact on Federal Standard

Data privacy laws recently signed into law in Colorado and Connecticut went into effect on July 1, 2023, adding to the growing patchwork of enforceable state privacy laws and regulations. These states join California and Virginia, whose laws have taken effect. However, on June 29, 2023, the Superior Court for the County of Sacramento issued a Tentative Ruling prohibiting California from enforcing the state's regulations supplementing the California Privacy Rights Act (CRPA) until March 29, 2024. The state initially scheduled the rules to take effect on July 1, 2023.

A number of states have new privacy laws that are scheduled to go into effect over the next 24 months, many of which became law in June 2023. Utah's law will take effect at the end of the year, while laws in Delaware, Florida, Iowa, Montana, Oregon, Tennessee and Texas will take effect in 2024 or 2025. Indiana's law takes effect on Jan. 1, 2026.

On June 7, 2023, Florida Gov. Ron DeSantis signed into law the Florida Digital Bill of Rights (SB 262), a wide-ranging privacy bill that includes enhanced protections for kids' data. The bill creates new prohibitions on online platforms that provide an online service, product, game or feature likely to be predominately accessed by children under 18 years old and accessible to children in Florida. These prohibitions include processing data that may result in substantial harm or privacy risk to children, using dark patterns, profiling and collecting precise geolocation data, though some exceptions exist. However, other than the new children protections, the Florida law applies to large tech platforms only.

In addition, Texas Gov. Greg Abbott signed into law on June 18, 2023, the Texas Data and Privacy Security Act (TDPSA). Like other states' privacy laws, the TDPSA provides consumer rights regarding how the industry may collect and use personal information. The TDPSA also has stringent requirements for "data brokers." Small businesses, as defined by the U.S. Small Business Administration (SBA), will be exempt. In addition, on June 13, 2023, Gov. Abbott signed the Securing Children Online Through Parental Empowerment (SCOPE) Act (HB 18), which takes effect on Sept. 1, 2024. The SCOPE Act seeks to protect children under age 18 on websites that allow them to create posts and interact with other users.

Meanwhile, other states with active legislative sessions continue to consider privacy-related legislation. For example, Massachusetts has been working on the Location Shield Act, which, if enacted into law, would impose the first-in-the-nation ban on all sales of Massachusetts residents' mobile phone location data.

As the number of state privacy laws grows, reaching consensus on a federal privacy bill that attempts to create one national standard could become more fraught politically for lawmakers whose state privacy laws could be preempted by a federal standard. Nevertheless, key congressional committees continue to negotiate provisions of a federal privacy bill and intend to reintroduce a modified version of the American Data Privacy and Protection Act (ADPPA) later this year.

A more palatable option may be to pursue narrow federal privacy bills such as children's privacy. Senate Majority Leader Chuck Schumer (D-N.Y.) continues to signal interest in bringing kids' privacy bills to the floor and recently told colleagues in a caucus-wide Dear Colleague letter that online internet safety legislation remains a near-term priority. President Joe Biden's State of the Union address in February 2023 called on Congress to enact "bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data these companies collect on all of us." Since then, however, other priorities – such as regulating artificial intelligence (AI) and boosting U.S. competitiveness with China – have taken precedence for Schumer.

Despite the delay, the Senate Committee on Commerce, Science, and Transportation is expected to mark up kids' privacy legislation such as the Kids Online Safety Act (KOSA) (S. 1409) and the Children and Teens' Online Privacy Protection Act (COPPA 2.0) (S. 1418) in the coming months. The Commerce Committee approved both bills last Congress. Again, however, the onslaught of new state privacy bills adopted in 2023 – and any conflicting provisions – could complicate or deter the federal legislative process. Moreover, the state bills – which could create a de facto children's privacy standard for the industry given the difficulty of applying different standards across state lines – create less urgency around a federal solution. House Committee on Energy and Commerce Chair Cathy McMorris Rodgers (R-Wash.) has yet to endorse these bills; she has previously emphasized the need for a comprehensive solution like the ADPPA over a piecemeal, narrow privacy bill approach.

Data Brokers

On June 5, 2023, the Office of the Director of National Intelligence (ODNI) declassified a January 2022 report on the use of "commercially available information" from data brokers by both U.S. intelligence services and foreign governments. The report concludes that commercially available information "clearly provides intelligence value, whether considered in isolation and/or in combination with other information, and whether reviewed by humans and/or by machines." The report included three recommendations for changes that the U.S. intelligence community should pursue to govern the use of commercially available information. This report will undoubtedly influence Congress' oversight of the process the federal government follows to collect and analyze commercially available information from data brokers that does not require a warrant or other processes.

Artificial Intelligence

Schumer Releases AI Framework

Senate Majority Leader Chuck Schumer on June 21, 2023, released his AI framework, the SAFE Innovation Framework, which establishes five major policy objectives: 1) security, 2) accountability, 3) foundations, 4) explain and 5) innovation. The Framework outlines the Majority Leader's vision of how the U.S. should harness AI's potential and protect society from its potential harms in legislation. The move comes as the European Union (EU) inches closer to adopting the EU AI Act, which would more aggressively govern the use of AI in products sold in the EU.

According to Schumer, AI poses an urgent threat, particularly as China races to lead the world in AI. To streamline the development of a policy response that aligns with the SAFE Innovation Framework, Schumer has tasked committees with developing bipartisan legislation, and he has convened a bipartisan group of non-committee chairs to assist with the effort, including Sens. Mike Rounds (R-S.D.), Todd Young (R-Ind.) and Martin Heinrich (D-N.M.). Schumer's decision to appoint off-committee leaders could streamline the arduous committee review process. Schumer also announced that in fall 2023, he plans to begin holding "AI Insight Forums" in which top AI experts will brief Congress on AI-related topics, including workforce, national security, privacy and liability, use-cases and risk management, and guarding against doomsday scenarios. This announcement comes after the Senate held a hearing on AI oversight on May 16, 2023. In that hearing, all three witnesses, including OpenAI CEO Sam Altman, agreed that Congress needed to act, as new developments in generative AI technology – from large language models to art generators – are advancing at breakneck pace.

Other lawmakers, including Senate Commerce Committee Chair Ted Cruz (R-Texas), have urged caution in the Senate's approach to AI. Cruz recently noted that "hesitation on such regulation has served Washington well in the past," but he also agrees with the national and economic security threat China poses if it dominates the world in AI.

Work on a comprehensive AI bill is currently ongoing. It is unclear if there is enough collective momentum in the Senate to adopt a new AI policy, however, Schumer's push gives the effort a priority within the Senate. While issues associated with AI extend beyond data privacy and security, these elements will be central components of any legislative proposal. In particular, AI systems used to monitor the performance and behavior of individuals may impact an individual's rights to data protection and privacy.

Privacy Lawsuit Filed Against OpenAI

A San Francisco-based law firm filed a class action lawsuit against OpenAI in the U.S. District Court for the Northern District of California on June 28, 2023. The lawsuit alleges that OpenAI stole personal information to train its AI models by scraping publicly available information from the internet, including that of children. Moreover, the lawsuit alleges that OpenAI provides no effective procedures to effectuate an individual's right to request a company delete any personal information of that individual. Many believe that when an AI model is trained using an individual's personal information, the personal information cannot be effectively deleted once it becomes part of the machine learning of the AI system. The class action – which includes 15 counts, including invasion of privacy on behalf of 16 plaintiffs – claims $3 billion in potential damages. The outcome of this lawsuit could significantly impact the AI industry that has developed leveraging current online data and could influence federal policy and regulation regarding privacy and AI.

Senators Continuing Work on Judiciary Committee's Subcommittee on Privacy, Technology, and the Law

Sens. Richard Blumenthal (D-Conn.) and Josh Hawley (R-Mo.), the chair and ranking member, respectively, of the Senate Committee on the Judiciary's Subcommittee on Privacy, Technology, and the Law, introduced on June 14, 2023, the No Section 230 Immunity for AI Act, bipartisan legislation that would clarify that Section 230 of the Communications Decency Act (47 U.S.C. § 230) will not apply to claims based on generative AI. Specifically, the bill would amend Section 230 by adding a clause that strips immunity from AI companies in civil claims or criminal prosecutions involving the use or provision of generative AI.

In addition, Sens. Blumenthal and Hawley sent a letter to Meta CEO Mark Zuckerberg addressing concerns over a possible "leak" of Meta's AI model, the Large Language Model Meta AI (LLaMA). The letter states that such a leak could lead to misuse in spam, fraud, malware, privacy violations, harassment and other wrongdoing and harm. The senators seek answers from Meta on how the company assessed the risk of releasing LLaMA, what steps the company took to prevent the abuse of the model and how Meta is updating its policies and practices based on its "unrestrained availability." This letter demonstrates increased congressional concern over the security of companies' AI models.

Senators Send Letter to Twitter Over Allegations of Privacy Violations

Sens. Elizabeth Warren (D-Mass.), Ed Markey (D-Mass.), Ron Wyden (D-Ore.) and Mazie Hirono (D-Hawaii) sent a letter to Twitter owner Elon Musk and new CEO Linda Yaccarino over allegations that Twitter violated its consent decree with the Federal Trade Commission (FTC) and "put consumer privacy and data security at risk." The catalyst for the letter seemed to be the high-profile resignations of Twitter's head of trust and safety, Ella Irwin, and Twitter's head of brand safety and advertising quality, A.J. Brown. According to the letter, "These departures, following [the resignations], raise concerns about Twitter's ability to comply with its legal obligations." Citing previous FTC actions against the social media platform in the past, the senators posed a series of questions over Twitter's obligations to its privacy and security assessments and request the company to reply by June 18, 2023. This oversight activity has been used more frequently in recent years to influence commercial or federal agency activities, especially in lieu of new federal privacy legislation.

Legislators Seek to Protect Americans' Data from Unfriendly Nations

Sens. Ron Wyden (D-Ore.), chair of the Senate Committee on Finance, and Cynthia Lummis (R-Wyo.) introduced legislation on June 14, 2023, seeking to protect Americans' data from being exploited by unfriendly nations and apply tough criminal and civil penalties to prevent employees of foreign corporations like TikTok from accessing U.S. data from abroad. The Protecting Americans' Data from Foreign Surveillance Act of 2023, which was also introduced in the House by Reps. Warren Davidson (R-Ohio) and Anna Eshoo (D-Calif.), directs the U.S. Department of Commerce, in consultation with other key agencies, to identify categories of personal data that, if exported, could harm U.S. national security. In addition, the bill directs the Commerce Department to compile a list of low-risk countries where data can be shared without restrictions, a list of high-risk countries where exports of sensitive data will be blocked, and create a system to issue licenses for data exports to nationals not on either list.

In addition to regulating bulk exports, the bill also regulates all exports of personal data by data brokers and firms such as TikTok directly to restricted foreign governments, parent companies in restricted foreign countries and persons designated on the Bureau of Industry and Security's (BIS) Entity List. The bill also exempts the new export rules data encrypted with National Institute of Standards and Technology (NIST)-approved technology and ensures the export rules do not apply to journalism and other First Amendment-protected speech. In addition, one of the legislation's sponsors, Sen. Marco Rubio (R-Fla.), sent a letter to U.S. Attorney General Merrick Garland, urging the U.S. Department of Justice (DOJ) to investigate whether the TikTok CEO Shou Zi Chew committed perjury when he testified under oath that the data of TikTok's American users was not stored in China. Since then, *Forbes* reported that TikTok stored some of its American users' most sensitive data, including Social Security numbers, in China, where it could be assessed by the Chinese Communist Party.

Legislators Introduce DELETE Act

Sens. Bill Cassidy, M.D. (R-La.) and Jon Ossoff (D-Ga.), along with Reps. Lori Trahan (D-Mass.) and Chuck Edwards (R-N.C.), introduced the Data Elimination and Limiting Extensive Tracking and Exchange (DELETE) Act on June 22, 2023, to protect Americans' private online data. The DELETE Act would create a system for individuals to request all data broker companies that collect personal data for commercial use delete any personal data the broker may have collected and not collect it in the future. The DELETE Act would direct the FTC to create an online dashboard that allows Americans to submit a one-time data deletion to registered data brokers. Under current law, individuals must request removal from each data broker to ensure their privacy is protected. This legislation would also create a "do not track list" to protect taxpayers from future data collection.

Senators Send Letter to Amazon Over Clinical Health Data

After reporting that patients seeking to enroll in Amazon Clinic Services, the company's "virtual healthcare storefront," Sens. Elizabeth Warren (D-Mass.) and Peter Welch (D-Vt.) sent a letter to Amazon's president and CEO Andy Jassy, requesting information on the types of data collected by Amazon Clinic and how Amazon is using the data it collects. Amazon Clinic advertises low-cost healthcare that is provided online, a service that is especially relevant to rural Americans, who may have to travel long distances to secure medical care. The FTC recently secured a $1.5 million penalty from telehealth provider GoodRx for failing to notify customers that the company disclosed customers' personal health data to third parties for advertising. This is the FTC's first enforcement action under the 2023 Health Breach Notification Rule, which was reported in the May 2023 Data Privacy and Security Report.

Castor, Dingell Lead Letters to Social Media Platforms Requesting Information About Protections for Children

In the wake of an advisory recently released by U.S. Surgeon General Vivek Murthy underscoring concerns that social media companies are not responsibly mitigating the risks and subsequent harms to kids on their platforms, a group of lawmakers took notice. On June 14, 2023, Reps. Kathy Castor (D-Fla.) and Debbie Dingell (D-Mich.) led 18 other members of the House in sending letters to social media companies requesting information regarding their platforms, algorithms and steps they take to mitigate harm to children online.

"Companies have a responsibility to mitigate the fundamental risks of their platforms on underage users. These protections should be inherent to the design of platforms and must prioritize the safety, health, and privacy of children and teens," the lawmakers concluded. "We all share a commitment to protecting kids online and the need for greater transparency from social media companies on the steps they are currently taking to achieve these goals. While Congress must pass a bipartisan, comprehensive data privacy law to protect all Americans online, we need to ensure that companies are adequately and responsibly protecting children and teens in the interim." The full text of the letters are posted on Meta, TikTok, Snapchat, YouTube, Twitter and Twitch.

EXECUTIVE AND DEPARTMENTAL UPDATES

Update on the EU-U.S. Data Privacy Framework

As reported in the April 2023 Data Privacy and Security Report, the U.S. and EU are continuing to work out details on a new transatlantic data transfer deal, with an expected deal announcement by mid-July 2023. President Joe Biden and European Commission President Ursula Gertrud von der Leyen first announced the deal, known as the EU-U.S. Data Privacy Framework, in March 2022. After Biden signed an Executive Order in October 2022 to implement the EU-U.S. Data Privacy Framework, U.S. officials have been working to finalize details that protect constituencies on both sides of the Atlantic. In particular, the U.S. had been working to add further safeguards for intelligence activities, mandating requirements for personal information, requiring the U.S. Intelligence Community to update their policies and procedures to reflect the new privacy and civil liberties safeguards, creating a multilayer mechanism for individuals from qualifying states and regional economic integration organizations to obtain independent and binding review and redress, and working with other federal agencies, including the Privacy and Civil Liberties Oversight Board, to review various policies and procedures. On July 3, 2023, the U.S. announced its fulfillment of its requirements.

As part of the final negotiations holding up the EU's adoption of the framework, the DOJ had to create a court called the Data Protection Review Court (DPRC). The DPRC will review cases brought by EU citizens who believe their data has been wrongly shared with the U.S. government. On May 23, 2023, the DOJ's Office of Privacy and Civil Liberties (OPCL) published in the *Federal Register* a System of Records Notice (CPCLO Order No. 001-2023 – OPCL System of Records Notice). OPCL intends to establish a system of records to capture matters reviewed and decisions made by the DPRC in response to complaints that allege violations of U.S. law related to signals intelligence activities. The European Parliament adopted a resolution implementing the Framework on May 11, 2023.

FCC Launches Privacy and Data Protection Task Force

Federal Communications Commission (FCC) Chairwoman Jessica Rosenworcel announced on June 16, 2023, the establishment of a new Privacy and Data Protection Task Force. This FCC staff working group will coordinate across the agency on the rulemaking, enforcement and public awareness needs in the privacy and data protection sectors. The group's work will include data breaches such as those involving telecommunications providers related to cyber intrusion, as well as supply chain vulnerabilities involving third-party vendors that service regulated communications providers.

Rosenworcel appointed FCC Enforcement Bureau Chief Loyaan A. Egal to lead the task force. FCC staffers from across the agency comprise the task force. These staffers manage topics such as enforcement, equipment authorization, data breach reporting requirements and undersea cables.

CFPB Releases Report on Chatbots in Consumer Finance

In a new report, the Consumer Financial Protection Bureau (CFPB) warns banks and consumers that the growing use of AI-powered chatbots in banking systems may not only provide false information but could also raise certain privacy and security risks. The report warns that "When chatbots are poorly designed, or when customers are unable to get support, the chatbots can cause widespread harm and customer trust can be significantly undermined." A few examples the CFPB raises with regard to potential privacy flaws is that chat logs may make it more difficult to fully protect the privacy and security of consumers' personal and financial information. Additionally, large language model-trained chatbots rely on training datasets that contain illegally obtained information about individuals. Privacy violations may occur when training data includes personal information that is then directly disclosed by the model through no fault of the affected individual. In the report, the CFPB encourages entities to review their legal obligations when deploying chatbots and other advanced technologies. This warning puts banks on notice that the CFPB will closely monitor the use of chatbots in the markets it regulates and could take regulatory action against violators.

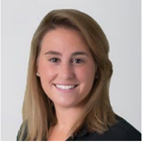
FTC Will Require Microsoft to Pay $20M Over Illegally Collected Personal Information from Children

The FTC announced that Microsoft will pay $20 million to settle charges that it violated the Children's Online Privacy Protection Act (COPPA) by collecting personal information from children who signed up for its Xbox gaming system without notifying their parents or obtaining their parents' consent, and by illegally retaining children's personal information. The proposed order filed by the DOJ on behalf of the FTC requires Microsoft to take several steps to bolster privacy protections for child users of its Xbox system. For example, the order will extend COPPA protections to third-party gaming publishers with whom Microsoft shares children's data. In addition, the order makes clear that avatars generated from a child's image and biometric and health information are covered by the COPPA Rule when collected with other personal data. A federal court must approve the order before it can go into effect. The COPPA Rule requires online services and websites directed to children under age 13 to notify parents about the personal information they collect and to obtain verifiable parental consent before collecting and using any personal information collected from children.

Contractors: Direct Employees to Remove TikTok from Personal Cell Phones, Other Devices

As published in a Holland & Knight alert on June 28, 2023, the Federal Acquisition Regulatory Council (FAR Council) recently issued an interim rule, FAR 52.204-27, which implements the Office of Management and Budget's (OMB) guidance prohibiting the use of TikTok on information technology used by federal agencies and contractors and expands the reach of the previous prohibition of TikTok on personal devices used in contract performance. The alert outlines the interim rule and discusses how contractors must direct their employees to remove TikTok from personal cell phones and other devices.

CONTACTS



Marissa C. Serafino
Associate
Washington, D.C.
202.469.5414
marissa.serafino@hklaw.com

Joel E. Roberson
Partner
Washington, D.C.
202.663.7264
joel.roberson@hklaw.com

Misha Lehrer
Senior Public Affairs Advisor
Washington, D.C.
202.469.5539
misha.lehrer@hklaw.com

Christopher DeLacy
Partner
Washington, D.C.
202.457.7162
chris.delacy@hklaw.com

Greg M. Louer
Partner
Washington, D.C.
202.469.5538
greg.louer@hklaw.com

Parker M. Reynolds
Summer Associate
Washington, D.C.
202.469-5606
parker.reynolds@hklaw.com