Holland & Knight

Data Privacy and Security Report: April 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 the authors or members of Holland & Knight's Data Strategy, Security & Privacy Team.

LEGISLATIVE UPDATES

The Growing State Privacy Law Patchwork and the Potential Impact on a National Privacy Standard

With the signing of Indiana's privacy bill into law on May 1, 2023, seven states have now adopted state privacy laws – California, Colorado, Connecticut, Indiana, Iowa, Utah and Virginia. Florida, Montana and Tennessee also have privacy bills pending with the governors for signature. Additional states may join this list, as New York and Texas legislatures have advanced comprehensive privacy bills during their legislative sessions. Moreover, Washington's governor signed into law the My Health My Data Act on April 27, 2023, which creates new restrictions on the collection and disclosure of "consumer health data" by companies in Washington or that are related to Washington residents. (See Holland & Knight's previous alert, "Washington State Imposes Far-Reaching Privacy Obligations for Consumer Health Data," May 2, 2023.)

These privacy laws will likely play a role in federal privacy bill negotiations, which have often been derailed over the preemption of state laws. 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 would be effectively unenforceable if the bill preempted – unless Congress were to carve out each state privacy law.[i] The U.S. House Committee on Energy and Commerce (E&C) leaders plan to reintroduce the American Data Privacy and Protection Act (ADPPA) from last Congress (or similar legislation) to establish a national online privacy standard. The ADPPA would provide privacy rights to individuals in states where no privacy law has been adopted. It is possible, however, given the number of new privacy laws, that Congress pivots to narrow privacy bills such as kids' privacy legislation.

House Energy and Commerce Continues Oversight Focus on Data Privacy

The House E&C Committee has held six privacy and data security hearings in 2023, three of which occurred in April. These hearings demonstrated bipartisan support for comprehensive privacy legislation, as well as interest in Big Tech oversight, regulating data brokers, increasing transparency and safeguards in the industry, instituting additional child privacy protections and encouraging data minimization to safeguard consumers' data.

- **FTC FY 2024 Budget:** On April 18, 2023, the E&C's Subcommittee on Innovation, Data, and Commerce held a hearing to review the Federal Trade Commission's (FTC) fiscal year (FY) 2024 budget request. The hearing featured the three Democratic FTC commissioners: Chair Lina Khan, Rebecca Slaughter and Alvaro Bedoya. Both Republican FTC seats on the five-member agency remain vacant. The FTC requested a $590 million for FY 2024, marking a $160 million increase from the FY 2023 enacted levels. During the hearing, Republicans expressed skepticism about the requested budget increase, accusing the agency of overstepping its jurisdiction in pursuit of a progressive enforcement agenda and wasting its resources. Conversely, Democrats praised the FTC's efforts to increase enforcement and create new rulemaking on commercial surveillance and junk fees. Several Democrats advocated for their own pieces of legislation, such as the Online Consumer Protection Act, Kids PRIVCY Act and the Consumer Equity Protection Act, all of which would expand the FTC's authority. The partisan views of the FTC demonstrate a divide that will continue to surface as Congress works towards stronger data privacy laws and seeks to determine what role the FTC should play in enforcing those laws.

- **National Data Privacy Standard:** The E&C's Subcommittee on Innovation, Data, and Commerce held a hearing on April 27, 2023, regarding the need for a national data privacy standard. Lawmakers discussed how consumers may not be covered by sector-specific laws in a way that is consistent with their expectations. By examining sector-specific data privacy regimes – such as the financial sector's Gramm-Leach-Bliley Act (GLBA), the healthcare sector's Health Insurance Portability and Accountability Act (HIPAA) and the education sector's Family Education Right and Privacy Act (FERPA) – the subcommittee and its witnesses sought to expose gaps in coverage that a piecemeal sector-specific approach has created for consumers.

- **Data Brokers:** The E&C's Subcommittee on Oversight and Investigations held a hearing, "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy," on April 19, 2023. Members discussed the collection and selling of personal data and how data brokers profit from that data, which could establish a record for future legislative action. The subcommittee and its witnesses conveyed three major takeaways: 1) data brokers with no consumer interface are collecting swaths of sensitive personal information, 2) there is a lack of transparency, and consumers have little understanding of data brokers' use of their personal information and 3) there is a growing need for a comprehensive national standard that empowers consumers and requires companies to make privacy the default.

Senators Introduce Legislation Focused on Kids' Safety Online

Sens. Richard Blumenthal (D-Conn.), Marsha Blackburn (R-Tenn.) and Lindsey Graham (R-S.C.) reintroduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act), and the U.S. Senate Committee on the Judiciary approved the bill on May 4, 2023. This bill seeks to bolster the existing federal framework governing the prevention of online sexual exploitation of children. First, the bill encourages the tech industry to take action to make the internet safer for kids online by amending Section 230 of the Communications Decency Act to remove blanket immunity for violations of laws related to online child sexual abuse material (CSAM). Second, the bill bolsters enforcement tools and provides civil recourse for survivors. Third, the bill brings together stakeholders through a National Commission on Online Child Sexual Exploitation Prevention, which would be responsible for developing voluntary best practices companies can take to prevent, reduce and respond to the online sexual exploitation of children. Senators unanimously reported the EARN IT Act out of the

Judiciary Committee last Congress, but the bill did not receive a vote on the Senate floor. Critics of the bill from the technology industry and civil rights groups still oppose the bill over censorship and cybersecurity concerns. Reps. Ann Wagner (R-Mo.) and Sylvia Garcia (D-Texas) plan to introduce companion legislation in the House of Representatives.

Similarly, Senate Majority Whip and Chair of the Senate Judiciary Committee Dick Durbin (D-Ill.) introduced the Strengthening Transparency and Obligation to Protect Children Suffering from Abuse and Mistreatment Act (STOP CSAM Act). The STOP CSAM Act would require mandatory child abuse reporting by federal grant recipients that provide services to children. The bill would also strengthen current CyberTipline reporting requirements, removing tech companies' discretion as to whether to report a planned or imminent child exploitation offense.

Additionally, Sens. Chris Murphy (D-Conn.), Brian Schatz (D-Hawaii), Tom Cotton (R-Ark.) and Katie Britt (R-Ala.) introduced the Protecting Kids on Social Media Act, which would require consent from parents of children ages 13-17 to access social media accounts and would prohibit users who are under the age of 13 from accessing platforms. Under the bill, online platforms would also be required to verify the age of all users. Sens. Blackburn and Blumenthal also recently reintroduced the Kids Online Safety Act, which would require platforms to design their products with children's safety in mind.

These bills represent a growing bipartisan effort to increase accountability and transparency in children's safety online, and more bills on child protections are likely to come. While passing comprehensive data privacy legislation would be an uphill battle due to politically charged issues subject to negotiation, a narrow child privacy and protection bill may have a better chance of passage.

Democrats Urge Administration to Confront the Influence of Big Tech During U.S. Trade Negotiations

A group of Democratic lawmakers sent a letter to U.S. Commerce Secretary Gina Raimondo and U.S. Trade Representative Katherine Tai warning negotiators to not let large tech companies influence provisions of the Indo-Pacific Economic Framework (IPEF). Members expressed concerns with the Framework's treatment of data privacy, artificial intelligence (AI) and antitrust matters. The lawmakers took issue with large technology platforms' pursuit of trade rules which, they argue, would allow borderless transmission of sensitive data online without congressional oversight.

TikTok Remains Top of Mind for Some Lawmakers

Sen. Thom Tillis (R-N.C.) and Rep. Dan Crenshaw (R-Texas) are leading a push to ban the use of TikTok by fellow lawmakers. In a letter to the Senate Committee on Rules and Administration and the House Committee on House Administration, the lawmakers urged the committees to "bar members of Congress from continued use of TikTok and take any other appropriate measures to mitigate the risks of this de-factor, spyware app." This letter comes after leaders in the U.S. Department of Defense (DOD) and the National Security Agency (NSA) briefed the House Committee on Armed Services' Subcommittee on Cyber, Innovative Technologies, and Information Systems on the cybersecurity risks posed to the United States by the Chinese-owned company.

Meanwhile, work continues on bills to address privacy and security concerns associated with TikTok. E&C Committee Chair Cathy McMorris Rodgers (R-Wash.), for instance, is developing a bill tailored specifically to TikTok. Sens. Mark Warner (D-Va.) and John Thune (R-S.D.) also continue negotiations behind the scenes to advance their bill, the RESTRICT Act (S. 686), which would grant the U.S.

Department of Commerce authority to block certain transactions involving foreign companies that threaten national security. The Biden Administration is supportive of this bill and is focused on identifying companies that may pose national security risks to America's networks and Americans' data. Efforts to prevent foreign adversaries from exploiting Americans' data and the technology supply chain – especially using social meta platforms and data brokers – will likely continue; however, it is unclear whether the RESTRICT Act will gain enough traction to become law.

Congress Requests Briefing with CFPB Following Data Breach of 250,000 Consumers

Leaders in the House and Senate requested further information from the Consumer Financial Protection Bureau (CFPB) following an employee forwarding the names and account numbers of more than a quarter of a million consumers to a personal email account. In a letter, Ranking Member of the Senate Committee on Banking, Housing, and Urban Affairs Tim Scott (R-S.C.) requested a briefing and expressed concerns about the CFPB's handling of data and the agency's data privacy practices. Similarly, Rep. Bill Huizenga (R-Mich.), the chair of the House Committee on Financial Services' Subcommittee on Oversight and Investigations, asked CFPB Director Rohit Chopra to testify in front of the subcommittee on the agency's "mitigation and remediation efforts, the scale of the breach, as well as efforts made to give the appropriate notifications."

EXECUTIVE AND DEPARTMENTAL UPDATES

Biden Administration Releases Joint Statement on AI

Recently, officials from the FTC, U.S. Department of Justice (DOJ), CFPB and Equal Employment Opportunity Commission (EEOC) released a joint statement outlining their commitment to enforce laws and regulations to promote innovation in automated systems. Specifically, the joint statement stated that these agencies "take seriously [their] responsibility to ensure that these rapidly evolving automated systems are developed and used in a manner consistent with federal laws, and each of our agencies has previously expressed concern about potentially harmful uses of automated systems." The joint statement pinpointed concerns regarding unlawful discrimination when using AI to perform tasks, make recommendations and form predictions.

Currently, federal efforts to address the threats posed by the rapid development and adoption of generative AI have been disjointed. In an effort to drive legislation that would create a regulatory framework for AI and support U.S. leadership in the technology, Senate Majority Leader Chuck Schumer (D-N.Y.) recently announced that he would spearhead a legislative push to create AI guardrails. Discussions to develop the contours of a bill are ramping up quickly, though still in a nascent stage.

HHS Issues Proposed Rulemaking on HIPAA Reproductive Healthcare Privacy

On April 13, 2023, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking (NPRM) to enhance the HIPAA Privacy Rule by "prohibiting the use or disclosure of protected health information (PHI) to identify, investigate, prosecute, or sue patients, providers and others involved in the provision of legal reproductive health care, including abortion." Comments on the proposed rule are due by June 16, 2023. For more information, please see Holland & Knight's previous alert, "HHS Proposes HIPAA Changes to Protect Reproductive Health Information," April 14, 2023.

DOJ Prepares for Data Flow Deal with the EU Despite Delays

In October 2022, the European Union (EU) and United States announced a goal to create a data privacy framework, with President Joe Biden signing an Executive Order to allow data transfers between the U.S. and the EU. The European Commission must also approve the data flow deal, but the approval has been delayed. The European Commission intended to approve the deal in March 2023, but approval was delayed because the DOJ has not finalized the Data Protection Review Court, a court that would be tasked with reviewing cases brought by citizens of the EU who believe their data has been wrongly shared with the United States government. Peter Winn, the DOJ's Chief Privacy and Civil Liberties Officer, provided a progress report regarding the court's creation at a recent Privacy Symposium. He indicated they are close to finalization: judges have been selected for the court, and the DOJ is waiting for clearance before announcing them.

ONC Proposes Updates to Information Blocking Regulations

HHS Office of the National Coordinator (ONC) for Health Information Technology published a Notice of Proposed Rulemaking called the "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Proposed Rule" (HTI-1 Proposed Rule). The HTI-1 Proposed Rule implements provisions of the 21st Century Cures Act (Cures Act) and arrives approximately three years after the ONC Cures Act Final Rule. The HTI-1 Proposed Rule, like its predecessor, aims to further advance interoperability, improve transparency and support the access, exchange and use of electronic health information. (See Holland & Knight's previous alert, "ONC Proposes Updates to Information Blocking Regulations," April 27, 2023.)

DIA Publishes RFI for AI Technical Assistance, IT Support

The Defense Intelligence Agency (DIA) published a request for information (RFI) seeking companies that can realize a DOD directive to stand up an AI capability by 2025. The DIA, whose mission is to produce, analyze and disseminate military intelligence for the DOD on foreign militaries and their operating environments, is seeking to identify sources, obtain new ideas and information pertaining to the state of the industry for providing technical assistance and information technology support to stand up an AI capability in 1) AI career development (training and recruitment) and 2) AI infrastructure and tools.

For additional defense-related information, please see the Holland & Knight Defense Situation Report: April 2023, April 27, 2023.

CONTACTS

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

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

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

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

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

Parker M. Reynolds
Public Affairs Advisor
Washington, D.C.
202.469-5606
parker.reynolds@hklaw.com

[i] The latest version of the ADPPA (H.R. 8152) carved out California's privacy laws from the bill's preemption provision. Section 404(b)(2)(R) - 404(b)(3).