Holland & Knight

Data Privacy and Security Report: November 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

End-of-Year Sprint

With an appropriations fight punted to the new year, lawmakers will likely spend the remainder of 2023 devoting attention to passing the National Defense Authorization Act (NDAA) and considering a potential supplemental appropriations bill to provide national security aid for Israel, Ukraine, Taiwan and the U.S. border.

Kids' Privacy Bills Stalled in Senate

Early November, Senate Committee on Commerce Chair Maria Cantwell (D-Wash.) announced plans to "hotline" privacy legislation in the Senate. Hotlining refers to a procedure in which a senator may expedite passage of a bill through unanimous consent. Any senator with concerns must object to the hotline and identify their concerns by providing an opportunity to resolve such concerns for the bill to move forward. She planned to hotline the following bills:

- Children and Teens Online Privacy Protection Act 2.0 (COPPA 2.0): Sponsored by Sens. Ed Markey (D-Mass.) and Bill Cassidy (R-La.), the bill would reform COPPA to prohibit online companies from collecting personal information from users who are 13 to 16 years old without their consent and ban targeted advertising to children and teens.
- Kids Online Safety Act (KOSA): Sponsored by Sens. Richard Blumenthal (D-Conn.) and Marsha Blackburn (R-Tenn.), the bill would impose a duty of care for digital services to prevent harm to younger users.

The Senate Commerce Committee favorably reported both bills in July 2023 during a markup. However, Cantwell postponed hotlining the bills in an effort to address remaining objections to KOSA regarding privacy and censorship concerns. The delay comes as public pressure to move the bill continues to mount. Most recently, a coalition of 200 kids' online safety advocates – which includes Common Sense Media, the American Psychological Association, Accountable Tech and the Eating Disorder Foundation – sent a letter to Senate Majority Leader Chuck Schumer (D-N.Y.) and Minority Leader Mitch McConnell (R-Ky.), calling on them to move the KOSA, "as well as strong privacy protections for kids and teens online, to the U.S. Senate floor for a vote by the end of the year."

It is unlikely, however, that a vote on COPPA 2.0 and KOSA would occur before the end of the year. Last year, both bills made it out of committee before ultimately failing to secure floor time for a vote.

Whistleblower Testimony Fans Flames for Kids' Online Safety Legislation

On Nov. 7, 2023, the Senate Committee on the Judiciary's Subcommittee on Privacy, Technology, and the Law held a hearing, "Social Media and the Teen Mental Health Crisis." In the hearing, Facebook's former director of engineering for protect and care testified to how social media algorithms push content to teens that promote bullying, drug abuse, eating disorders and self-harm. The need for stronger privacy parental controls and increased transparency as companies profit from children's data was a core tenet of the whistleblower's testimony.

During the hearing, Senate Majority Whip and Judiciary Committee Chair Dick Durbin (D-Ill.) stated: "In the Senate Judiciary Committee, after some graphic hearings where parents and victims came forward and told us what had happened to them online, we decided to take action. We passed six bills related to this issue – child sexual abuse and similar issues. … Six bills waiting for a day on the calendar. Six bills waiting for a national debate. … They put real teeth in enforcement too and I think that is why they have gone nowhere. Big Tech is the big kid on the block when it comes to this issue and many other issues before us. That's the reality."

Soon after that hearing, the Judiciary Committee announced another hearing scheduled for Jan. 31, 2024, on child online exploitation in which the CEOs of five major social media companies will testify.

Sen. Wyden to Oppose Confirmation of New NSA/Cyber Command Leader

On Nov. 30, 2023, Sen. Ron Wyden (D-Ore.) announced he will place a hold on the nomination of Lt. Gen. Timothy Haugh as leader of the National Security Agency (NSA) and U.S. Cyber Command, citing complaints that defense and intelligence officials have refused to make public information received in 2021 about the NSA purchasing and using location data collected on Americans. He has vowed to block the confirmation until the NSA discloses whether it is buying Americans' location data web browsing records. He stated in a statement placed in the Congressional Record: "The American people have a right to know whether the NSA is conducting warrantless domestic surveillance of Americans in a manner that circumvents the Fourth Amendment to the Constitution. Particularly as Congress is currently debating extending Section 702 of the Foreign Intelligence Surveillance Act, Congress must be able to have an informed public debate about the scope of the NSA's warrantless surveillance of Americans." Haugh's nomination has enjoyed broad support, but with the hold, Gen. Paul Nakasone, the current head of the NSA and Cyber Command, will continue to serve with his term past due.

This hold comes as Congress considers the NDAA, which includes a short-term extension through April 19, 2024, of Section 702 of the Foreign Intelligence Surveillance Act (FISA), a controversial tool that allows the government to collect data from foreigners abroad. The authority was set to expire at the end of 2023. On Dec. 8, 2023, Wyden voted against a procedural vote on the NDAA in opposition to the Section 702 reauthorization.

Sen. Cortez Masto Reintroduces Three Privacy Bills

On Nov. 16, 2023, Sen. Catherine Cortez Masto (D-Nev.) reintroduced three privacy bills, including:

1. The DATA Privacy Act is a comprehensive privacy bill that aims to strengthen protections for American online consumers while ensuring large corporations implement data security and privacy protections. Specifically, the bill would require businesses to provide users with an easily accessible opt-out method for personal data collection or sharing.

2. The Promoting Digital Privacy Technologies Act, which is also sponsored by Sen. Deb Fischer (R-Neb.), would require the National Science Foundation (NSF) to support research into privacy enhancing technologies (PET). The bill also requires the National Institute of Standards and Technology (NIST) to work with academic, public and private sectors to establish standards for the integration of PET into business and government.
3. The Internet Application I.D. Act aims to improve Americans' digital security by requiring operators of internet websites and mobile applications to disclose if the applications being used by consumers have been developed or store data within China or are under the control of the Chinese Communist Party.

The path forward for these bills is unclear, given that they have failed to receive enough bipartisan support in past years to advance. Nevertheless, Holland & Knight will monitor these bills in 2024, as some of the bills' provisions could be included in other legislation.

Involuntary Facial Recognition Bill Introduced

On Nov. 29, 2023, Sens. John Kennedy (R-La.) and Jeff Merkley (D-Ore.) introduced the Traveler Privacy Protection Act, which seeks to safeguard Americans from involuntary facial recognition screenings at airports. The bill would repeal the Transportation Security Administration's (TSA) authorization to use facial recognition and prevent the agency from further exploiting the technology and storing travelers' biodata. The co-sponsors of the bill fear that although TSA calls its plans to voluntarily implement facial scans at more than 430 U.S. airports, passengers are largely unaware of their ability to opt out, and TSA does not effectively display notices to inform passengers of that option. The bill would 1) require explicit congressional authorization in order for TSA to use facial recognition technology going forward, 2) immediately ban the TSA from expanding its pilot facial recognition program and 3) require TSA to end its pilot facial recognition program and dispose of facial biometrics.

Data Collection from Servicemembers Is Under the Microscope

Sen. Roger Wicker (R-Miss.) recently wrote a letter to Secretary of Defense Lloyd Austin that took issue with private firms collecting and selling troves of hypersensitive data on active-duty soldiers and their family members that can then openly be bought online by foreign adversaries. Wicker advocated for strict privacy protections on soldiers' personal devices. Wicker's letter references a recent study from Duke University that examined the risks presented to U.S. national security by this dynamic. The issue has picked up bipartisan interest, as the NDAA conference report includes a provision that requires the Comptroller General of the United States to provide a briefing to the House and Senate Committees on Armed Services, as well as the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, on the U.S. Department of Defense's (DOD) efforts to protect personal information of its personnel from exploitation by foreign adversaries. Additionally, Sen. Bill Cassidy (R-La.) introduced the Protecting Military Service Members' Data Act – legislation that would prevent data brokers from selling lists of military personnel to adversarial nations such as China and Russia.

EXECUTIVE AND DEPARTMENTAL UPDATES

CFPB Issues Proposed Personal Finance Data Rule

On Nov. 15, 2023, the Federal Communications Commission (FCC) adopted new rules to protect consumers against scams that aim to commandeer their cell phone accounts by strengthening protections against SIM swapping and port-out fraud. SIM swapping refers to bad actors convincing a victim's wireless carrier to transfer the victim's service from the victim's cell phone to a cell phone in the bad actor's possession. Port-out fraud takes place when the bad actor, posing as the victim, opens an account with a carrier other than the victim's current carrier. The bad actor then arranges for the victim's phone number to be transferred (or "ported out") to the account with the new carrier controlled by the bad actor. SIM swapping and port-out fraud compromises a consumer's data and personal information. Under the new rules, wireless providers will be required to immediately notify customers whenever a SIM change or port-out request is made on a customer's account and take additional steps to protect customers. The FCC also adopted a Further Notice of Proposed Rulemaking to seek comment on ways to harmonize these rules with existing FCC Customer Proprietary Network Information (CPNI) and Local Number Portability rules.

U.K., U.S. Unveil the World's First AI Cyber Guidelines

On Nov. 26, 2023, the U.K.'s National Cyber Security Center and U.S. Cybersecurity and Infrastructure Security Agency unveiled the world's first artificial intelligence (AI) cyber guidelines, which are backed by 18 countries, including Japan, Israel, Canada and Germany. It's the latest move on the international stage to get ahead of the risks posed by AI as companies race to develop more advanced models, and systems are increasingly integrated into government and society.

The guidelines aim to ensure security is a "core requirement" of the entire life cycle of an AI system and are focused on four themes: secure design, development, deployment and operation. Each section has a series of recommendations to mitigate security risks and safeguard consumer data such as threat modeling, incident management processes and releasing AI models "responsibly."

Judges Named to Data Protection Review Court

The United States-United Kingdom Data Bridge went into effect on Oct. 12, 2023, following the U.K. publishing its Data Protection (Adequacy) (United States of America) Regulations 2023 as reported in the Data Privacy and Security Report: October 2023. As part of the executive order President Joe Biden signed in October 2022 to implement the EU-U.S. Data Privacy Framework, the U.S. Department of Justice (DOJ) established a Data Protection Review Court. The court will review cases filed by European Union residents alleging the U.S. government violated American regulations by digitally surveilling them. On Nov. 14, 2023, the Biden Administration named eight judges to serve on the court, all of whom are experienced with data privacy and national security laws as dictated by the executive order. The judges include:

- Rajesh De, a former general counsel at the National Security Agency
- Eric Holder, 82nd U.S. attorney general
- Mary DeRosa, a professor at Georgetown University Law Center and a former National Security Council legal adviser
- Thomas Griffith, a former judge on the U.S. Court of Appeals for the D.C. Circuit

- James Baker, director of the Syracuse University Institute for Security Policy and Law and a former chief judge on the U.S. Court of Appeals for the Armed Forces
- James Dempsey, senior policy adviser at the Stanford Program on Geopolitics, Technology and Governance, former member of the U.S. Privacy and Civil Liberties Oversight Board and former senior counsel for the Center for Democracy and Technology
- David Levi, president of the American Law Institute and former member of the Presidential Commission on the Supreme Court
- Virginia Seitz, former assistant attorney general for the DOJ's Office of Legal Counsel

CFPB Seeks to Balance Development of New Banking Products and Privacy Protections

On Nov. 29, 2023, Consumer Financial Protection Bureau (CFPB) Director Rohit Chopra discussed the agency's October 2023 notice of proposed rulemaking (NPRM) restricting how financial institutions handle consumer data. The "Personal Finance Data Rule" would give consumers the right to control their data, including allowing consumers to more easily switch providers and more conveniently manage accounts from multiple providers. CFPB anticipates that the rule will accelerate a shift toward open banking, where consumers would have control over data about their financial lives and would gain new protections against companies misusing their data. Testifying in front of the House Committee on Financial Services, Chopra recognized that the new rule's data protections will likely make it more difficult for banks to anonymize customer data to develop new products. He emphasized that advanced AI has made it easier to reidentify consumers; however, CFBP is aware of banks' concerns and is looking for ways to address them. Comments on the proposed rule are due by Dec. 29, 2023, and a final rule is expected in fall 2024.

STATE UPDATES

CPPA Rolls Out Draft ADMT Regulations

On Nov. 27, 2023, the California Privacy Protection Agency (CPPA) released its draft automated decision-making technology (ADMT) regulations that would govern how state residents' data could be used in AI and automated decision-making technologies. For example, the draft regulations propose requirements for businesses using ADMT to profile consumers by tracking a consumer's location, evaluating consumers' personal preferences and interests, or using facial-recognition technology or automated emotion assessment to analyze consumers' behavior. The proposed regulations would implement consumers' right to opt out of and access information about businesses' uses of ADMT, as provided for by the California Consumer Privacy Act (CCPA). The CPPA Board provided feedback on the proposed regulations at its Dec. 8, 2023, board meeting, and the CPPA expects to begin formal rulemaking next year.

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