Michael Kans' Technology Policy Update
15 May 2019
By Michael Kans, Esq.

FTC Oversight Hearing

On May 8, the House Energy and Commerce Committee's Consumer Protection and Commerce Subcommittee heard from the entire Federal Trade Commission (FTC) at a hearing titled "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security."

The witnesses at the hearing were, of course:

- Chair Joseph Simons
- Commissioner Noah Joshua Phillips
- Commissioner Rohit Chopra
- Commissioner Rebecca Kelly Slaughter
- Commissioner Christine S. Wilson

Subcommittee Chair Jan Schakowsky (D-IL) noted that recent media reports have indicated the FTC is considering record-breaking fines against Facebook, and she asserted that the publicly known information underscores the need for comprehensive privacy legislation. She said that while she appreciates the FTC's work in the Facebook case, a single large fine will not meaningfully address the privacy issues confronting consumers. Schakowsky said this includes the fact that the FTC lacks the tools it needs to protect consumers in today's economy. She said the FTC needs increased funding and Administrative Procedure Act rulemaking authority to restore the confidence of consumers in today's digital and bricks and mortar marketplace. Schakowsky said the FTC should be able to pursue multiple investigations large and small and noted the agency lacks the authority to seek civil fines for most initial violations of the FTC Act. She said worse still, the FTC only has 40 full-time staff devoted to privacy and data security, and in contrast to the United Kingdom's Information Commissioner's Office (ICO), which has 500 employees for a country about one-fifth the size of the U.S. in terms of population. Schakowsky observed that unlike other recent Administrations, the FTC has yet to appoint a Chief Technologist and only has five employees identified as technologists. She said Energy and Commerce Democrats feel they have an obligation to provide a solid piece of legislation that protects consumer privacy and have begun conversations with committee Republicans. Schakowsky expressed her hope the legislation would be bipartisan and informed by collaboration with the FTC.

Subcommittee Ranking Member Cathy McMorris Rodgers (R-WA) said she was glad the FTC was before the subcommittee to discuss its vital missions of protecting consumer privacy and promoting competition and innovation. She said in the 21st Century, Americans start and end their days with products that save time, keep us informed and connected, and help them work. McMorris Rogers stated that Americans share their information throughout each and every day with the Internet marketplace and asserted that this "free-flow of information" drives much of the technology innovation and growth in the U.S. She claimed that Americans make choices every day to be connected, and when they do, they must be able to trust that their privacy will be protected. McMorris Rodgers said consumers deserve to know how their data is being collected, used, and shared with. She claimed that there "shouldn't be so many surprises, and these protections should

change depending on which state we're in." She noted a recent survey in which 75% of respondents said privacy protections should be the same wherever they go. McMorris Rodgers said this is why she has been advocating for a national data privacy standard that 1) does not leave consumers' privacy "vulnerable in a patchwork;" 2) increases transparency and targets harmful practices like Cambridge Analytica; 3) improves data security practices; and 4) is workable for U.S. innovators and small businesses. She stated that the FTC is the "main cop on the beat" to promote privacy standards and transparency and hold companies accountable. McMorris Rodgers said the FTC's mission is to protect consumers and promote innovation, and she asserted that Republicans' four principles for a data privacy law are in line with that mission, notably protecting consumers from concrete harm, empowering their choices, and promoting new technologies. McMorris Rodgers said she "remains ready and willing to work with colleagues on this committee for a bi[partisan solution that puts consumers and their choices first." She said "various proposals" have called for the FTC to receive additional funding and authority but expressed her skepticism about Congress delegating broad authority to the FTC or any agency. McMorris Rodgers called for policymakers to be mindful of the complexities of this issue as well as the lessons learned from previous grants of rulemaking authority to the FTC. She asserted that the subcommittee must examine how the FTC has utilized its existing rulemaking authority regarding privacy and data security.

Chair Frank Pallone Jr (D-NJ) contended that the FTC needs more funding and authority to fight those committing frauds and scams on consumers. He said the same is true of privacy and data security, which is a daunting task considering companies monitor every move Americans make, what they view online, whom they talk to, and what they say or do in their homes. Pallone asserted that given the Facebook and Cambridge Analytica and Equifax scandals, consumers have little reason to believe that these companies will protect and respect their data. He asserted the FTC can and must be doing more to protect consumers, and Congress should give the agency the tools it needs to be more effective. Pallone said this starts with resources; the FTC has fewer employees today than in the 1980's when the internet did not exist. He claimed the agency also needs authority to prevent privacy abuses from happening in the first place and that companies ensure the personal data entrusted to them. Pallone noted the agency lacks the authority to fine companies for initial violations, and in order to deter, the agency must be able to fine in the first instance. He stated that to make matters worse, there are no strong and clear federal privacy laws and regulations that establish a baseline for how companies collect, use, share, and protect consumer information. Pallone stated that Congress must pass strong, comprehensive privacy legislation that should give consumers control over their personal data, including giving consumers the ability to access, correct, and delete their personal information.

Ranking Member Greg Walden (R-OR) stated that privacy does not mean the exact same thing to every American. He expressed his agreement with McMorris Rodgers "who outlined the vast benefits consumers get from the use of their information online." Walden stated that "[w]e cannot lose sight of the tremendous benefits consumers get from the use of data – access to top-tier journalism, affordable and quickly delivered products, telehealth and research initiatives, and much more." He claimed that "[h]ere in the U.S., we have a thriving startup ecosystem and a regulatory environment that enables small businesses to grow and compete, in no small part because of the free flow of information…[a]nd, as a result, companies innovate, create new jobs, and offer consumers options and convenience." Walden said that "I believe it is important that we work together toward a bipartisan federal privacy bill…[a]nd we are ready and willing to tackle crafting such a bill." He asserted that "[a] federal privacy bill must set one national standard…[and] [a]llowing a patchwork of state laws will not only hurt innovation and small businesses but will limit consumers options online." Walden asserted that "[w]e must enhance security for consumers…[and] [c]ompanies must have

reasonable practices in place to protect consumer information." He contended that "[w]e must increase transparency – consumers deserve to know how their information is collected, used, and shared…[a]nd we must improve accountability." Walden stated that "I believe the FTC is the right agency to enforce a new privacy law with appropriate safeguards and process improvements to ensure strong, consistent enforcement." He noted that "[s]ome have suggested that the quick answer is more money, more rulemaking authority, and more employees…[but] [t]here is no quick fix."

Simons explained that

> Our primary legal authority in this space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial practices. But Section 5 is an imperfect tool. For example, Section 5 does not allow the Commission to seek civil penalties for first-time privacy violations. It does not allow us to reach non-profits and common carriers, even when their practices have serious implications for consumer privacy and data security. These limitations have a critical effect on our ability to protect consumers, which is why we urge Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers.

Senate Banking Hearing on Consumer Privacy

On May 7, the Senate Banking, Housing, and Urban Affairs Committee held its first hearing on data privacy in the 116th Congress titled "Privacy Rights and Data Collection in a Digital Economy" with the following witnesses:

- German Marshall Fund of the United States Senior Fellow Peter Chase
- PwC US Privacy and Consumer Protection Leader Jay Cline
- Pinboard Founder Maciej Ceglowski

Chair Mike Crapo (R-ID) said that "[o]n February 13, [Ranking Member Sherrod Brown (D-OH)] and I invited feedback from the public on the collection, use and protection of sensitive information by financial regulators and private companies in light of the immense growth and use of data for a multitude of purposes across the economy." He stated that "[b]uilding on that effort, today the Committee will take a closer look at the European Union's General Data Protection Regulation, or GDPR, and other approaches to data privacy, including the impact on the financial services industry and how companies collect and use information in marketing and decision-making related to credit, insurance or employment." Crapo stated that "[e]ach witness brings a unique perspective on the practical implications of implementing and complying with new data privacy laws; what has worked and what has not worked to give individuals more control over their data; and considerations for the Committee as it explores updates to federal data privacy laws within the Banking Committee's jurisdiction." He noted his "concerns about big data collection go back as far as the creation of the [Consumer Financial Protection Bureau], which was collecting massive amounts of personal financial information without an individual's knowledge or consent." He asserted that "[c]onsumers deserve to know what type of information is being collected about them, what that information is being used for and how it is being shared." Crapo stated that "[f]inancial regulators are not the only ones engaged in big data collection; private companies are also collecting, processing, analyzing and sharing considerable data on individuals." He said that "[a] complete view of what data is collected, the sources of that data, how it is processed and for what purposes, and who it is being shared with is vital to individuals exercising their rights." Crapo stated that "[p]eople should also be assured

that their data will be reflected accurately, and have the opportunity to opt out of it being shared or sold for marketing and other purposes."

Ranking Member Sherrod Brown (D-OH) said that "I'm excited to be working in a bipartisan way with Chairman Crapo on protecting Americans' sensitive personal data –an issue everyone agrees is important." He said that "[t]here's a lot of data floating around that can be compiled and analyzed in creative ways to make shockingly accurate predictions about our lives." Brown stated that "[w]hat you think of as your "personal data" isn't limited to bank passwords and credit scores…[and] even if you don't have a Facebook account, Facebook builds a shadow profile of your activities, interests, and preferences from digital bread crumbs spread by your friends and associates online." He contended that '[t]here's a common saying that "if you're not paying for the product, then you are the product.'" He asserted that "[s]ervices that appear free make money from your personal data…[and] [i]t's not easy for consumers to protect themselves." He claimed that 'buyer beware' is not a helpful warning, since most people cannot afford to protect themselves by opting out of internet services just like they cannot opt out of banking products with arbitration clauses in them." Brown stated that "[i]f we don't take this seriously, a handful of big tech corporations and financial firms will continue to strong arm customers into sharing their most intimate details." He said that "in addition to talking about ownership and control of our data today, I hope we can also talk about where government needs to step in and create rules around the appropriate uses of personal data -regardless of whether a customer opts-in." Brown added that "[t]he Banking Committee is only responsible for one slice of the data ecosystem –I hope to work with the Chairman of the Banking Committee as well as the Chairs and Ranking Members of the other committees of jurisdiction to set some commonsense rules on the use of Americans' sensitive personal data."

Cline said that his "testimony today will examine the experience of US financial institutions (FIs) with the European Union (EU) General Data Protection Regulation (GDPR)…an experience marked by large-scale technical and organizational change to afford new privacy rights to EU residents in an evolving regulatory environment." He stated that "GDPR caused many US FIs operating in Europe to undertake their largest-scale privacy program initiatives in two decades." Cline said that "[b]eginning after the ratification of the GDPR in April 2016 and generally accelerating a year later, these initiatives often rivaled the scale of US FIs' earlier mobilizations to prepare for the Privacy Rule of the Gramm-Leach-Bliley Act (GLBA) and other related US data privacy laws and regulations." He said that "[a]s a result, US FIs generally used all of the GDPR's two-year grace period to prepare for the law's "go live" date in May 2018." Cline said that the "GDPR introduced several new obligations on US FIs:

- New requirements on data-subject rights most affected retail banks and direct insurers – because of their direct exposure to fulfilling data-subject requests (DSRs) –and least affected commercial banks, re-insurers, payment-card companies, and asset-management companies that generally had indirect exposure to DSRs.
- New requirements on data privacy program accountability by comparison most affected larger, diversified groups of companies that had to allocate more resources to accommodate their business variations and least affected more homogenous FIs.

Cline stated that "[t]he effects of the GDPR requirements included increases in headcount, changes in information systems, and alterations in products and services."

NIST AI RFI and FDA AI Framework

The National Institute of Standards and Technology (NIST) has released a request for information (RFI) to meet a requirement in the February 2019 executive order (EO) "Maintaining American Leadership in Artificial Intelligence (AI)" "to create a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies (Plan)." NIST wants to "understand the current state, plans, challenges, and opportunities regarding the development and availability of AI technical standards and related tools, as well as priority areas for federal involvement in AI standards-related activities." In its press release, NIST explained that comments are due on May 31, 2019 and it "will host a workshop on May 30, 2019, at its Gaithersburg, Maryland, campus."

The EO requires NIST to "issue a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies" within 180 days, and this RFI is the first public step in the process. NIST stated that it "will develop the Plan in a manner that fulfills the objectives of the E.O. and is consistent with relevant provisions of the Office of Management and Budget (OMB) Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," and NIST's mission to promote U.S. innovation and industrial competitiveness." In terms of next steps, NIST stated it "expects to develop a draft Plan on which it will seek comment from the public and Federal agencies."

Through this RFI, NIST "seeks to understand the:

- Current status and plans regarding the availability, use, and development of AI technical standards and tools in support of reliable, robust, and trustworthy systems that use AI technologies;
- Needs and challenges regarding the existence, availability, use, and development of AI standards and tools; and
- The current and potential future role of Federal agencies regarding the existence, availability, use, and development of AI technical standards and tools in order to meet the nation's needs.

NIST explained that "[f]or purposes of this Plan, AI technologies and systems are considered to be comprised of software and/or hardware that can learn to solve complex problems, make predictions or solve tasks that require human-like sensing (such as vision, speech, and touch), perception, cognition, planning, learning, communication, or physical action. Examples are wide-ranging and expanding rapidly...[which] include, but are not limited to, AI assistants, computer vision systems, automated vehicles, unmanned aerial systems, voicemail transcriptions, advanced game-playing software, facial recognition systems as well as application of AI in both Information Technology (IT) and Operational Technology (OT)."

Additionally, NIST is not the only agency moving forward on AI. In an initiative unrelated to NIST's RFI, the Food and Drug Administration (FDA) has released a discussion paper "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback" "that describes the FDA's foundation for a potential approach to premarket review for artificial intelligence and machine learning-driven software modifications." FDA explained that it's "traditional paradigm of medical device regulation was not designed for adaptive artificial intelligence and machine learning technologies...[and] [u]nder the FDA's current approach to software modifications, the FDA anticipates that many of these artificial intelligence and machine learning-driven software changes to a device may need a premarket review."

The agency stated that "[i]n this framework, the FDA introduces a "predetermined change control plan" in premarket submissions...[and] [t]his plan would include the types of anticipated modifications—referred to as the "Software as a Medical Device Pre-Specifications"—and the associated methodology being used to implement those changes in a controlled manner that manages risks to patients —referred to as the "Algorithm Change Protocol." The FDA stated that "[t]he proposed regulatory framework could enable the FDA and manufacturers to evaluate and monitor a software product from its premarket development to postmarket performance...[and] [t]his potential framework allows for the FDA's regulatory oversight to embrace the iterative improvement power of artificial intelligence and machine learning-based software as a medical device, while assuring patient safety."

Other Hearings

"Review of the FY2020 Budget Request for the FCC & FTC" – Senate Appropriations/Financial Services and General Government
"Election Security" – House Administration

Further Reading

"President Trump Is Spending $20 Billion on an Aircraft Carrier. The Navy Wanted That Money for Cybersecurity" – *Time*
"A Mysterious Hacker Group Is On A Supply Chain Hijacking Spree" – *WIRED*
"Has Los Angeles County just reinvented voting?" – *NBC*
"Verizon, T-Mobile, Sprint, and AT&T Hit With Class Action Lawsuit Over Selling Customers' Location Data" – *Motherboard*