Cyber Update
3 April 2019
By Michael Kans

Senate Privacy Hearing

The Manufacturing, Trade, and Consumer Protection Subcommittee of the Senate Commerce, Science, and Transportation Committee held another hearing on a federal privacy statute while Members are said to be working on a bipartisan bill. This hearing focused on how a federal privacy framework might affect small businesses. The chair and ranking member of the subcommittee expressed their commitment to working in a bipartisan way on a yet-to-be released federal privacy statute, but their opening statements marked out significantly different positions suggesting the distance still to be traveled on reaching consensus on how a new federal privacy regime should work. Moreover, having a hearing that focuses on how small businesses would be affected by a privacy statute suggests the most stringent requirements may be aimed at "big tech" (e.g. Facebook or Google.) However, it is also possible that exemptions for small businesses may be utilized by larger businesses as a means of limiting exposure to enforcement authority.

The witnesses appearing before the subcommittee were:

- Consumer Reports Privacy and Technology Policy Director Justin Brookman
- National Association of Realtors Technology Policy Committee Vice Chair Nina Dosanjh
- Silver Star Communications Chief Financial Officer Jefferson England
- Engine Advocacy and Research Foundation Executive Director Evan Engstrom
- KC Tech Council President Ryan Weber

Subcommittee Jerry Moran (R-KS) said more and more questions have arisen from allegations of unfair and deceptive practices conducted by a variety of companies handling of consumer's personal information. He said the subcommittee has focused on privacy issues going back into the previous Congress and has heard from the primary agency with jurisdiction over federal privacy issues, the Federal Trade Commission (FTC). Moran remarked that last fall, all five FTC Commissioners testified before the subcommittee on legislative options to protect consumers from harmful business practices and "bad actors." He said that the subcommittee's information gathering from industry, consumer advocacy groups, academics, and government agencies are intended to inform the subcommittee's legislative efforts to bolster consumer protection. Moran said the implementation of the General Data Protection Regulation (GDPR), passage of the California Consumer Privacy Act (CCPA), and the likelihood of other states passing privacy statutes, it is clear the U.S. needs a federal data privacy law that provides clarity in an increasingly complicated regulatory environment. He said to that end, he has been working with Ranking Member Richard Blumenthal (D-CT) and other Republicans and Democrats on the full committee, including Chairman Roger Wicker (R-MS) and Senator Brain Schatz (D-HI), to identify responsible federal privacy standards that provide clear and effective protection to consumers while also providing regulatory certainty to businesses in the interest of creating jobs and promoting innovation and competition in the global economy. Moran said that the hearing would focus on how a fragmented regulatory landscape affects small and new businesses, recognizing they have fewer resources for compliance. He noted the importance of acknowledging they will use consumer data in different ways and hence will have different liability. Moran said he wanted to know from the witnesses how the FTC's new

authorities should account for the size and scope of a business processing consumer data while also factoring in the sensitivity of that information and consumer harms associated with those practices.

Ranking Member Richard Blumenthal (D-CT) expressed his gratitude to Moran for his work on privacy issues and said there is a significant and committed team of Senators working to move forward on bipartisan legislation, including Wicker and Schatz. He declared that the issue of privacy is of paramount importance. Blumenthal said he and Senator Amy Klobuchar (D-MN) also both serve on the Senate Judiciary Committee, which recently held a hearing on privacy issue. He expressed his hope that the two committees could work together on this issue. Blumenthal noted that one year ago this month, the world learned that Cambridge Analytica had illicitly stolen data on tens of millions of Facebook users to manipulate U.S. elections. He characterized these revelations as "wakeup call for the American public" that "shifted our relationship with big tech." Blumenthal said anyone who thinks her privacy is sacrosanct or protected is fooling herself. He said Americans need a privacy bill of rights no less stringent than the people of California will have under CCPA and than the people of Europe have under GDPR. Blumenthal said our smartphones are the most sophisticated tracking devices known to humans, and people do not care whether it is a tech giant or a small business mining their data; consumers want to be able to choose how that information is used or shared. Blumenthal said more companies like DuckDuckGo that protect privacy and are profitable. He asserted Congress can set a baseline floor that establishes privacy as a bill of rights and a business value, promoting a market that enables companies to compete in offering the best privacy friendly services rather than "dumbing them down or punishing them." Blumenthal said he looks forward to crafting rules that accommodate the needs of small businesses "but we must raise the bar not lower it."

Chairman Roger Wicker (R-MS) expressed his appreciation for the work of Moran and Blumenthal and noted Ranking Member Maria Cantwell (D-WA) shares their goals as well. He said that federal privacy legislation must be crafted on a bipartisan basis. Wicker said that any privacy statute should protect consumers and promote economic growth, especially for small businesses, the "engine of so much job creation."

Brookman said "[a]s an initial matter, it is important to keep in mind the fundamental reason we are debating this issue: the United States lacks any sort of comprehensive framework to protect personal privacy." He said that the FTC "has brought a number of important privacy and security cases over the past twenty years under its general purpose consumer protection authority, but its legal authority and resources are extremely limited." Brookman stated that "[t]he considerable majority of its privacy cases have been under its *deception* authority, meaning the company had to affirmatively mislead consumers about their privacy practices." He claimed that "[a]s a result, privacy policies tend to be extremely expansive and vague, providing very little in the way of meaningful information…[and] [c]urrent law imposes few other checks on the collection and dissemination of our personal information."

Brookman said "[i]n developing privacy legislation, there are a number of elements that could be included to accommodate the relative lack of resources and sophistication of small businesses:

- *Thresholds*. First, a law could waive compliance with some subset of consumer protections for companies under a certain size.
- *Exempting Pseudonymous Online Data from Access and Deletion Requirements*. Other provisions in a thoughtful privacy law could make compliance easier for small companies. For example, while a privacy law should apply broadly to a wide range of information — including online data associated only with a cookie or IP address — exempting certain data

from access requests would ease the burden of compliance, prevent illegitimate access to personal information in shared environments, and incentivize companies to maintain in less identifiable forms.

- *Put Compliance Obligations on Tracking Companies — Not Websites*. Privacy law can also be constructed to transfer compliance obligations from small publishers to the large data broker and tracking companies who are the primary target and concern of the law.
- *Provide for Data Portability and Interoperability to Allow Small Providers to Compete with Larger, Incumbent Players*. Finally, strengthening consumer agency with regard to their own data can also promote competition and market choice. Data portability and interoperability requirements can accomplish both important policy goals by giving consumers control over their data while helping small businesses compete with big companies.

Dosanjh detailed "Key Principles For Federal Privacy Legislation:"

- *Establish Uniform Standards for Businesses and Equal Protection for Consumers*. Federal law should provide consumer data with uniform legal protections across all industries. Any federal data privacy legislation should apply requirements to all industries that handle personal data and not exempt certain sectors of the economy from providing consumer data protection.
- *Direct Statutory Obligations for All Service Providers Handling Consumer Data*. Effective consumer protection regulations cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Expecting small businesses to effectively negotiate contract terms surrounding privacy and data security on their own against large corporations with extensive legal departments is simply not a viable option.
- *Transparency and Customer Choice*. Consumers deserve to know what categories of personal data that businesses collect and how that data is generally used by them. Federal data privacy law should provide the regulatory flexibility necessary to ensure that transparency in privacy policies is provided to consumers without unnecessarily burdening businesses with requirements to seek consumer consent when they are continuing to use data based on reasonable consumer expectations.
- *Accountability for Business's Own Actions*. Privacy legislation should not include terms that could potentially expose businesses to liability for the actions or non-compliance of a business partner.
- *Uniform Nationwide Standard and Enforcement for Data Privacy*. Congress should create a sensible, uniform federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides.
- *Reasonable FTC Enforcement Authority*. The FTC should have the appropriate authority to enforce comprehensive privacy regulations. NAR appreciates that the FTC employs a scalable reasonableness approach that determines the appropriateness of business practices in light of the size of the business and the sensitive nature of the data they process under Section 5 of the FTC Act. Any future privacy legislation should ensure that the FTC continues to employ flexibility in their implementation of reasonable privacy standards that will permit the Commission to enforce such regulations fairly and equitably to ensure businesses' compliance with them and to promote robust consumer protection.

House OGR Examines CRA's Data Security

On March 26, the House Oversight and Government Reform Committee's Economic and Consumer Policy Subcommittee held a hearing titled "Improving Data Security at Consumer Reporting

Agencies." A number of congressional committees continue to focus on the discrete realm of data security particular to consumer reporting agencies (CRA) after the massive Equifax breach in 2017. If Congress is unable to arrive at comprehensive data security and breach notification legislation either as part of privacy legislation or a standalone bill, then it is possible there could be targeted legislation increasing the Federal Trade Commission (FTC) or Consumer Financial Protection Bureau's (CFPB) oversight and enforcement authority over CRAs.

These witnesses testified before the subcommittee:

- Government Accountability Office Financial Markets and Community Director Michael Clements
- George Mason University Research Fellow Jennifer Huddleston
  U.S. PIRG Consumer Campaigns Director Mike Litt
- Federal Trade Commission Bureau of Consumer Protection Director Andrew Smith

Subcommittee Chair Raja Krishnamoorthi (D-IL) said that the subcommittee would examine consumer reporting agencies (CRA) with an eye to improving their data security in light of the September 7, 2017 Equifax breach of 148 million Americans' sensitive personal information. He said that while many Americans became aware of the sensitive information held by CRAs, it is still not clear how many CRAs operate in the U.S. Krishnamoorthi stated that the Consumer Financial Protection Bureau (CFPB) estimates there are more than 400. He remarked the causes of the data breach have been investigated and exposed, and it is the job of Congress to prevent more Americans from having their sensitive personal information stolen. Krishnamoorthi noted that through Gramm-Leach-Bliley, Congress directed the Federal Trade Commission (FTC) to implement data security rules for CRAs, and the agency did so with the Safeguards Rule, which requires CRAs to take reasonable steps to protect sensitive data. He asserted the FTC has limited recourse in enforcing the rule, cannot levy fines for first violations, can only recover money from CRAs if harm to consumers can be shown, and often waits years for the negative effects of a breach to surface. Krishnamoorthi said the Government Accountability Office (GAO) will testify on their recommendations to give the FTC penalty authority to prevent breaches and to protect data security. He contended that enhancing FTC penalty power to enforce data security follows the model set by regulation in the banking industry, which has thus far avoided large, harmful data breaches.

Government Accountability Office (GAO) Financial Markets and Community Director Michael Clements said

> In 2006, we suggested that Congress consider providing FTC with civil penalty authority for its enforcement of GLBA's privacy and safeguarding provisions." We noted that this authority would give FTC a practical tool to more effectively enforce provisions related to security of data and consumer information. Following the 2008 financial crisis, Congress introduced several bills related to data protection and identity theft, which included giving FTC civil penalty authority for its enforcement of GLBA. However, in the final adoption of these laws, Congress did not provide FTC with this authority. Since that time, data breaches at Equifax and other large organizations have highlighted the need to better protect sensitive personal information. Accordingly, we continue to believe FTC and consumers would benefit if FTC had such authority, and we recommended in our February 2019 report that Congress consider providing FTC with civil penalty authority for the privacy and safeguarding provisions of GLBA to help ensure that the agency has the tools it needs to most effectively act against data privacy and security violations.

Clements added that

> Statute requires CFPB to consider risks posed to consumers in the relevant product and geographic markets in its risk-based supervision program. In addition, federal internal control standards state that agencies should identify, analyze, and respond to risks related to achieving defined objectives. This can entail considering all significant internal and external factors to identify risks and their significance, including magnitude of impact, likelihood of occurrence, nature of the risk, and appropriate response. In light of the Equifax breach, as well as CFPB's acknowledgment of the CRA market as a higher-risk market for consumers, it is important for CFPB to routinely consider factors that could inform the extent of CRA data security risk such as the number of consumers that could be affected by a data security incident and the nature of potential harm resulting from the loss or exposure of information. In our February 2019 report, we recommended that CFPB assess whether its process for prioritizing CRA examinations sufficiently incorporates the data security risks CRAs pose to consumers, and take any needed steps identified by the assessment to more sufficiently incorporate these risks. CFPB neither agreed nor disagreed with our recommendation.

Clements noted that "[i]n its February 2019 report on strengthening the oversight of CRAs, the GAO recommended:

- Congress should consider providing the FTC with civil penalty authority for the privacy and safeguarding provisions of the Gramm-Leach-Bliley Act to help ensure that the agency has the tools it needs to most effectively act against data privacy and security violations.
- The Director of CFPB should identify additional sources of information, such as through registering CRAs or leveraging state information, that would help ensure the agency is tracking all CRAs that meet the larger participant threshold.
- The Director of CFPB should assess whether its process for prioritizing CRA examinations sufficiently incorporates the data security risks CRAs pose to consumers, and take any needed steps identified by the assessment to more sufficiently incorporate these risks."

FTC Bureau of Consumer Protection Director Andrew Smith said "where Congress has provided the Commission with rulemaking authority related to data security, we will use that authority when warranted." He added that "the Commission recently proposed changes to the Safeguards Rule under the GLB Act, and is soliciting public comment on those proposed amendments." Smith said that "[t]he Safeguards Rule, originally issued in 2002, requires financial institutions within the FTC's jurisdiction – including CRAs– to implement reasonable, process-based safeguards to protect personal information in their control." He said that "[t]hese proposed revisions are intended to retain the process-based approach of the original Rule while providing financial institutions with more certainty as to the FTC's data security expectations."

Smith said the FTC "agrees with the GAO's recommendation that providing the FTC with civil penalty authority for violations of GLB's Safeguards Rule would give the FTC a practical enforcement tool that would benefit consumers." He asserted that "[b]eyond GLB, however, the Commission has long called for comprehensive data security legislation that would give the agency additional tools." Smith stated that "[i]n particular, the FTC supports data security legislation that would provide the agency with three essential additional authorities:

(1) the ability to seek civil penalties effectively to deter unlawful conduct,
(2) jurisdiction over non-profits and common carriers, and

(3) the authority to issue targeted implementing rules under the Administrative Procedure Act (APA).

George Mason University Research Fellow Jennifer Huddleston said she wanted to focus "the following three points:

1. Regulators should avoid an expansive theory of harm in their approach to data security.
2. The FTC has been the main agency for enforcing data security and data privacy, and its flexible approach has allowed innovation to flourish while still redressing consumer harm.
3. Policy solutions should be narrowly tailored and should focus on the unique position of credit reporting agencies."

Huddleston stated that "[n]ot only can a broad definition of harm associated with the breach of personal information deter innovation, it can also be nearly impossible to enforce." She said that as a result of its case-by-case approach, "the FTC has built a "common law of consent decrees" when it comes to data breaches and generally eschews more formal rulemaking or adjudication." Huddleston said that "[w]hile this approach prevents many of the harms to innovation that could come from top-down rulemaking, it also lacks clear guidance for private actors who seek to remain compliant and creates uncertainty in what may arise if practices are challenged." She said that "[i]n general, this flexible approach of ex-post case-by-case enforcement has resulted in balancing the need for consumer redress with the benefits of innovation." She added that "the FTC should strive to improve this approach through enforcement actions that develop a greater certainty around data security procedures that can protect consumers while continuing to avoid rigid, all-encompassing theories of harm that might actually deter future solutions and do little to nothing to improve the current state of data security."

Senate Armed Services Delves Into DIB Cybersecurity

On March 26 the Senate Armed Services Committee's Cybersecurity Subcommittee held a hearing entitled "Cybersecurity Responsibilities of the Defense Industrial Base." The hearing follows a mid-March report released by the Secretary of the Navy after he requested "an independent Cybersecurity Readiness Review following the loss of significant amounts of Department of the Navy data." The report's authors stated

> The Secretary of the Navy was correct to question if the current cybersecurity governance structure was optimally focused, organized, and resourced. We find it is not. What follows are best practices and solutions that can put the [Department of the Navy] on the right path.

The witnesses appearing before the subcommittee were:

- MITRE National Security Sector Senior Vice President and General Manager William LaPlante
- Aerospace Industries Association Vice President John Luddy
- The Lucrum Group Chief Executive Officer Christopher Peters
- Progeny Systems Corporation Chief Technology Officer Michael P. MacKay

Chair Mike Rounds (R-SD) said that since the reporting of the breach of a contractor for the Naval Undersea Warfare Center in June 2018, the Department of Defense (DOD) "has been shocked into action." He asserted that the "truth" is that adversaries have been breaching our contractors for a much longer time by stealing our design information and intellectual property. Rounds noted that thieves have not targeted the DOD itself but rather "its vulnerable contractor base." He declared

that this espionage will never be stopped entirely and it is unlikely that it "can be negotiated away or deterred." Rounds said exfiltration must be made more difficult. He said the DOD cannot afford to continue leaking valuable design secrets to China and Russia, "effectively subsidizing their own defense developments." Rounds said "it is incredibly clear the status quo is not working." He claimed the Pentagon's efforts have been "disjointed" and a "reemphasis of current policies." Rounds acknowledged that the Navy has started to audit its contractors for compliance with their cybersecurity requirements. Rounds referred to the Navy's Cybersecurity Readiness Review, which includes several recommendations for improved collaboration and communication between the Navy and their contractors to mitigate cyber threats. He said he looks forward to understanding how the Navy will implement the recommendations. Rounds said the Office of the Secretary of Defense has reemphasized the National Institute of Standards and Technology's (NIST) cybersecurity standard, and the Pentagon stood up the Protecting Critical Technology Task Force headed by Major General Thomas Murphy, which is taking a wide ranging approach to possible solutions to proving contractor cybersecurity. However, he noted that the concerns of the Defense Industrial Base (DIB) must be considered as ever more stringent cybersecurity standards will drive smaller, more innovative firms away from contracting with the Pentagon. Rounds registered his reservations about cybersecurity checklists, which do not help entities prioritize risks.

Ranking Member Joe Manchin (D-WV) characterized the subject of the hearing as "a critical national security problem, namely the hemorrhaging of technology know-how from the U.S. industry and academia to adversaries, chiefly China, which enables the rapid progression of their military capabilities." He said the U.S. knows China is using cyber-hacking and coercive transfer agreements from U.S. companies to acquire U.S. intellectual property, which undermines the U.S. economy and ultimately erodes national security. Manchin remarked because it remains easier for hackers to penetrate networks than for defenders to prevent penetration, there are no simple solutions. He said he was encouraged that the Congress, DOD, and the private sector are finally facing the issues confronting the U.S. Manchin said it is imperative to improve the cybersecurity of smaller DIB companies, which are vital parts of the DOD's supply chain and sources of innovation, but he noted that many of these companies lack the resources to defend themselves and the DOD data they hold. Manchin declared it is crucial that this problem be solved.

MITRE National Security Sector Senior Vice President and General Manager William LaPlante said "let me offer some thoughts about some areas in which there might be some useful progress in this area, recognizing that there is no silver bullet and that none of these is going to be a panacea:

- Critical to a successful path forward, I believe, is the need to bend the cost curve on cybersecurity. We need to find ways to make cybersecurity architectures less expensive for the defense industrial base to implement.
- Another option that has been discussed – and was among the questions posed by the subcommittee in its invitation – relates to making the kinds of Continuous Diagnostic and Mitigation (CDM) products that the "Dot Gov" agencies are required by DHS to employ, also available to the defense industrial base.
- One concept that I think has particular promise, which Under Secretary of Defense for Acquisition and Sustainment Ellen Lord in fact has advocated exploring, is the idea of one or more cloud environments, operated under auspices of DOD, that would be specifically tailored to the needs of the defense industrial base.
- One additional thing I would emphasize here is the need for the committee to look beyond just cybersecurity to also consider the broader challenges associated with the nation's supply chain. I realize this may extend the discussion beyond the writ of this subcommittee.

Aerospace Industries Association Vice President John Luddy said "[i]n August 2015, DOD implemented Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." He said that "[w]ith this rule, DOD significantly increased the range of information that could be defined as covered defense information (CDI) – and thus needing protection – to nearly everything that a major defense contractor uses to perform contracts for DOD." Luddy stated that "[a]s a result, as specific DOD customers – the Army or Air Force, for example – determine and identify which unclassified information must be protected on contractor networks and in communications between the DOD and the industry supply chain, there has been a tendency to over-protect mundane or basic information with complicated marking requirements – there are over 100 categories of CUI in the National Archives Records and Administration (NARA) CUI Registry, and the guide to marking CUI is 41 pages long." Luddy stated that "the absence of a unified DOD approach to cybersecurity policy…has led to different customers within DOD adding requirements beyond the DFARS requirement for contract compliance, the National Institute for Standards and Technology (NIST) Special Publication 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.'" He stated that "[t]his too often occurs without any engagement with industry regarding the feasibility and costs associated with enhanced, agency-specific measures. This lack of uniformity complicates the landscape and adds significant ambiguity as companies are expected to comply with a burgeoning list of Service-unique requirements, resulting in segmented infrastructure, limited visibility and duplication of resources within contractor networks.

FTC Requests Privacy Information From Broadband Providers

Last week, the Federal Trade Commission (FTC) "issued orders to seven U.S. Internet broadband providers and related entities seeking information the agency will use to examine how broadband companies collect, retain, use, and disclose information about consumers and their devices" according to the agency's press release. The FTC is seeking information on the following "companies' privacy policies, procedures, and practices:"

- AT&T Inc.
- AT&T Mobility LLC
- Comcast Cable Communications doing business as Xfinity
- Google Fiber Inc.
- T-Mobile US Inc.
- Verizon Communications Inc.
- Cellco Partnership doing business as Verizon Wireless

The FTC explained that it "is initiating this study to better understand Internet service providers' privacy practices in light of the evolution of telecommunications companies into vertically integrated platforms that also provide advertising-supported content…[because] [u]nder current law, the FTC has the ability to enforce against unfair and deceptive practices involving Internet service providers."

The FTC is seeking the following information:

- The categories of personal information collected about consumers or their devices, including the purpose for which the information is collected or used; the techniques for collecting such information; whether the information collected is shared with third parties; internal policies for access to such data; and how long the information is retained;
- Whether the information is aggregated, anonymized or deidentified;

- Copies of the companies' notices and disclosures to consumers about their data collection practices;
- Whether the companies offer consumers choices about the collection, retention, use and disclosure of personal information, and whether the companies have denied or degraded service to consumers who decline to opt-in to data collection; and
- Procedures and processes for allowing consumers to access, correct, or delete their personal information.

Bill Introduced To End PATRIOT Act Surveillance

Last week, Senators Ron Wyden (D-OR) and Rand Paul (R-KY) and Representatives Justin Amash (R-MI) and Zoe Lofgren (D-CA) introduced the "Ending Mass Collection of Americans' Phone Records Act" "to permanently end the National Security Agency's (NSA) scandal-plagued program to surveil Americans' phone records" according to their press release. Earlier this month, the *New York Times* quoted a top aide to House Minority Leader Kevin McCarthy (R-CA) in an article, claiming that the NSA is no longer using authority under the Foreign Intelligence Surveillance Act (FISA) that was exposed by former NSA contractor Edward Snowden. McCarthy's national security adviser Luke Murry made these claims during a *Lawfare* podcast.

The bill would permanently remove the NSA's authority to restart the program. Congress will be faced with a FISA deadline in December when three FISA authorities expire:

- Section 215 of the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001" (P.L. 107-56) aka the business records exception in 50 U.S.C. §1861 that permits orders compelling the production of "any tangible thing" "relevant" to foreign intelligence, international terrorism, and counter-espionage investigations.
- Section 206 of the USA PATRIOT ACT aka the roving wiretap exception in 50 U.S.C. §1805(c)(2)(B) that allows for surveillance even when a subject changes phones.
- Section 6001 of the "Intelligence Reform and Terrorism Prevention Act of 2004" (P.L. 108-458) aka the lone wolf exception in 50 U.S.C. §1801(b)(1)(C) that allows for a more streamlined evidentiary showing under FISA when a foreign national is alleged to be engaged in international terrorism absent a defined link to an international terror organization.

Lawmakers will need to grapple with how and whether to reauthorize these surveillance authorities, and the pending reauthorization may be used as a leverage point by opponents of these surveillance programs to hold up unrelated cyber or data security priorities as happened in 2015 when expiration of FISA's authorities, including the three mentioned above, was used to block consideration of cybersecurity information sharing legislation.

HUD Charges Facebook with Housing Discrimination

The Department of Housing and Urban Development (HUD) filed a charge of discrimination against Facebook, following a six-month investigation launched last August. HUD alleges that "Facebook unlawfully discriminates based on race, color, national origin, religion, familial status, sex, and disability by restricting who can view housing-related ads on Facebook's platforms and across the internet." The agency also asserted that "Facebook mines extensive data about its users and then

uses those data to determine which of its users view housing-related ads based, in part, on these protected characteristics." Facebook could face fines of more than $20,000 per violation if HUD succeeds in proving its case before an administrative law judge or in federal court.

HUD's charge comes a week after Facebook and a number of housing rights groups settled a related discrimination suit with the tech giant committing to changes. Media reports indicate that HUD is also investigating other large tech platforms like Google and Twitter, meaning that HUD may be bringing additional cases alleging violations of federal anti-discrimination housing laws.

A Facebook spokesperson was quoted in the *Washington Post* as saying the company was "surprised by HUD's decision, as we've been working with them to address their concerns and have taken significant steps to prevent ads discrimination." The spokesperson claimed that talks broke down when HUD pushed for too much access to Facebook data: "[w]hile we were eager to find a solution, HUD insisted on access to sensitive information — like user data — without adequate safeguards." The spokesperson added that "[w]e're disappointed by today's developments, but we'll continue working with civil rights experts on these issues."

In its charging document, HUD claimed that Facebook

- "[D]iscriminated by making dwellings unavailable because of race, color, religion, sex, familial status, national origin or disability."
- "[D]iscriminated in the terms, conditions, or privileges of the sale or rental of dwellings because of race, color, religion, sex, familial status, national origin or disability."
- "[M]ade, printed, or published – or caused to be made, printed, or published – notices, statements, or advertisements with respect to the sale or rental of dwellings that indicated preferences, limitations, or discrimination because of race, color, religion, sex, familial status, national origin or disability, or that indicated an intention to make such a distinction."
- "[S]elected media or locations for advertising the sale or rental of dwellings that denied persons information about housing opportunities because of race, color, religion, sex, familial status, national origin or disability."
- "[R]efused to publish advertising for the sale or rental of dwellings because of race, color, religion, sex, familial status, national origin or disability."
- "[R]equired different charges or terms for advertising the sale or rental of dwellings because of race, color, religion, sex, familial status, national origin and disability."

The National Fair Housing Alliance (NFHA), Fair Housing Council of Greater San Antonio (FHCGSA), Fair Housing Justice Center of New York (FHJC), and Housing Opportunities Project for Excellence, Inc. of Miami (HOPE, Inc.) filed suit in the U.S. District Court for the Southern District of New York in March 2018. The plaintiffs contended that "Facebook first provides the option for advertisers to exclude families with children and women from receiving advertisements, as well as users with interests based on disability and national origin…[and] [t]hen Facebook approves and permits advertisers to publish these ads in a discriminatory manner without consumers ever knowing they have been excluded."

A settlement was announced on March 19, 2019, and the plaintiffs claimed "Facebook will be making 8 big changes, positioning itself to be a pacesetter in advancing fair and equitable platforms, products and services and making the digital marketplace safer spaces for consumers:

- Facebook will establish a separate advertising portal for creating housing, employment, and credit ("HEC") ads on Facebook, Instagram, and Messenger that will have limited

targeting options, to prevent discrimination. Click here to see additional requirements for the HEC portal.

- Facebook will create a page where Facebook users can search for and view all housing ads that have been placed by advertisers for the rental, sale, or finance of housing or for real estate related transactions (such as appraisals and insurance), regardless of whether users have received the housing ads on their News Feeds.
- Facebook will require advertisers to certify that they are complying with Facebook's policies prohibiting discrimination and all applicable anti-discrimination laws.
- Facebook will provide educational materials and features to inform advertisers about Facebook's policies prohibiting discrimination and anti-discrimination laws.
- Facebook will meet regularly with the Plaintiffs and their counsel to report on and discuss the implementation of the terms of the settlements.
- Facebook will permit the Plaintiffs to engage in testing of Facebook's ad platform to ensure the reforms established under the settlements are implemented effectively.
- Facebook will work with NFHA to develop a training program for Facebook's employees on fair housing and fair lending laws.
- Facebook will engage academics, researchers, civil society experts, and civil rights/liberties and privacy advocates (including plaintiffs) to study the potential for unintended bias in algorithmic modeling used by social media platforms.

In August 2018, the U.S. Department of Justice (DOJ) filed A Statement of Interest in this case and noted that "[t]he United States frequently files Statements of Interest in cases concerning the applicability and interpretation of federal law in which it has enforcement interests." The DOJ noted that "HUD served an administrative complaint against Facebook for conduct similar to that alleged" in the plaintiffs' suit.

OIG Finds DEA May Have Overstepped Its Legal Authority In Bulk Data Collection

Last week, the Department of Justice's (DOJ) Office of the Inspector General (OIG) released its a review "of the Drug Enforcement Administration's (DEA) use of its administrative subpoena authority under 21 U.S.C. § 876(a) to collect or exploit 'bulk data.'" The OIG found that the DEA may have exceeded its legal authority to use its administrative subpoena authority under two programs and has been buying access to the bulk metadata of a telecommunications company alleged to be AT&T. At the very least, the OIG took issue with the lack of legal analysis as to whether these programs complied with the DEA's authority because the agency's construction of these authorities was "uniquely expansive" and suggested that there may be adequate legal grounds on which the programs could be challenged in court.

The Department of Justice (DOJ) Office of the Inspector General (OIG) announced today the release of a report examining the Drug Enforcement Administration's (DEA) use of its administrative subpoena authority under 21 U.S.C. § 876(a) to collect or exploit "bulk collections" of data.

The OIG explained that "Section 876(a) authorizes the DEA to issue administrative subpoenas, without court or other approval outside the agency, requiring the production of records that are "relevant or material" to certain drug investigations…[and] [a] "bulk collection" of data is a collection of a significant amount of data that is unrelated to an individual, group, or entity that is the target of an investigation."

The OIG explained that "Program A is a federal interagency data analysis program spearheaded by the DEA…[and] [f]rom the 1990s until mid-2013, as part of Program A, the DEA issued "non-target-specific" subpoenas to multiple telecommunications service providers to amass an extremely large collection of bulk telephone call records ("Collection 1")." The OIG stated that "[t]he Collection 1 subpoenas were "nontarget-specific" in that they were not directed at or related to particular identifiable investigations or targets." The OIG explained that the DEA issued subpoenas under this program to telecommunications companies for "records for all calls made from the United States over a recipient company's telecommunications network to countries that the DEA determined had a 'nexus to drugs.'" Additionally, the OIG explained that "telephone metadata" was also provided to the DEA but "the content of any calls or subscriber information."

The OIG stated that "Program B involved the use of administrative subpoenas from 2008 to 2013 to collect bulk purchase data for a particular good or service sold by selected vendors…[that] were issued periodically to selected vendors of the particular good or service and required production of customer information for each purchase of the good or service." The OIG stated that "[t]he DEA then queried the responsive Program B bulk purchase data provided by the vendors against various law enforcement databases to identify any matches, or "hits," in order to identify potential targets for further investigation." The OIG remarked that "[i]n September 2013, following inquiries from the OIG regarding Program B, the DEA stopped issuing administrative subpoenas in connection with this program."

The OIG stated that "Program C is a contractual service program, initiated by a non-DOJ government entity in 2007, under which a telecommunications service provider maintains and analyzes its own collection of bulk telephone metadata for billions of calls to produce expedited or advanced telephone analytical products in response to target-specific administrative subpoenas from law enforcement agencies, including DEA…[but] Program C does not include the content of calls." The OIG stated that "[a]mong other things, upon receiving an administrative subpoena, the provider can analyze its own bulk data collection to generate reports that identify unique connections to target phone numbers." The OIG stated that "[t]he provider maintains and queries the bulk collection; the DEA's administrative subpoenas for Program C products are issued for particular identifiable investigations or targets…[a]lthough this program is not one that the DEA owns, the DEA is a major customer for Program C products." The OIG stated that "Program C remains active."

The OIG "found that the DEA (and the Department with respect to Program A, Collection 1) failed to conduct a comprehensive legal analysis of the DEA's use of its administrative subpoena authority to collect or exploit bulk data before initiating or participating in any of the three programs." The OIG "found this failure troubling with respect to Program A, Collection 1 and Program B because these programs involved a uniquely expansive use of Section 876(a) authority to collect data in bulk without making a prior finding that the records were, in the language of that statutory provision enabling DEA's subpoena authority, "relevant or material" to any specific defined investigation." The OIG noted that "[s]everal published court decisions have clearly suggested potential challenges to the validity of the DEA's use of its statutory subpoena power in this expansive, non-targeted manner…[and] [w]e also found the absence of a robust legal review troubling because the DEA utilized the bulk data collected by means of Program A, Collection 1 and Program B."

The OIG added that DEA agents using programs A and C were told not to refer to the programs in affidavits, pleadings and other related documents, thus denying knowledge of this program to federal and state prosecutors, leading to possible *Brady* violations against defendants to whom

exculpatory evidence must be given. However, the OIG noted that so-called "parallel construction" is not inherently inappropriate, but it "should not be used to prevent prosecutors from fully assessing their discovery and disclosure obligations in criminal cases." The OIG stated that "[w]hile the DEA has denied misusing parallel construction in this manner, we found some troubling statements in the DEA's training materials and other documents, including that Program A investigative products cannot be shared with prosecutors."

The OIG "made 16 recommendations to the DEA to address the issues and concerns identified during our review, including the following:

- Before initiating or reinstating a "bulk collection" program by use of non-target - specific administrative subpoenas, the DEA should conduct a rigorous written legal assessment that specifically addresses whether 21 U.S.C. § 876(a) authorizes the issuance of non-targeted subpoenas for exploratory or target development purposes, and the permissible conditions under which such bulk data may be shared with other federal agencies for non-drug purposes.
- The DEA should issue a final legal opinion and updated policy on Program C and its permissible uses.
- The DEA should modify the electronic request form for Program A products to require more particularized documentation of the information to establish RAS and certification that the request pertains to a drug investigation. The DEA should develop legally supportable criteria for retention of Program B data collected by use of administrative subpoenas, and policies for the disposition of such bulk data.
- The DEA and other participating federal agencies should conduct periodic audits, on a set schedule, of an appropriate sample of Program A product requests to confirm, by tracking to the investigation from which the request originated, that there was an adequate particularized factual basis sufficient to establish RAS that the target number was relevant or material to an ongoing drug investigation.
- The Department should undertake a comprehensive review of "parallel construction" policies and practices with respect to Program A and Program C investigative products to ensure that these policies and practices do not conflict with the government's discovery and disclosure obligations in criminal cases, or Department policy on this subject, and that the Department's and DEA's guidance and training materials on this subject be clarified as warranted.

UK Oversight Board Finds No Progress on Huawei's Software Development; EU Charts A Different Course

The United Kingdom (UK) and the European Union (EU) sent opposing signals on the security of Huawei's systems for critical technology systems. A UK advisory board issued another negative assessment of the Chinese company's security and software development, while the EU put in place a process by which member states and the EU would assess the security risks associated with different companies in building out the continent's 5G networks. These developments occurred against the backdrop of continued U.S. pressure for allies and other nations to ban Huawei for alleged security risks that would benefit China and detriment other nations. So far, only Australia has agreed to ban Huawei.

Last week, the fifth annual report from the UK's Government Communications Headquarters' (GCHQ) Huawei Cyber Security Evaluation Centre Oversight Board (Board) was released, and the Board found that Huawei has failed to address the issues turned up in last year's report. Notably,

in its 2018 report, the Board stated "[d]ue to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated." In this year's report, the Board stated that "[n]o material progress has been made on the issues raised in the previous 2018 report."

The Board stated that its work "has continued to identify concerning issues in Huawei's approach to software development bringing significantly increased risk to UK operators, which requires ongoing management and mitigation." The Board asserted that it "continues to be able to provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK" and "advises that it will be difficult to appropriately risk-manage future products in the context of UK deployments, until the underlying defects in Huawei's software engineering and cyber security processes are remediated." The Board stated that it "has not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation programme that it has proposed as a means of addressing these underlying defects." The Board explained that it "will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC…[and] can only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term."

In a press release, the European Commission (EC) announced its recommendations on "a set of concrete actions to assess cybersecurity risks of 5G networks and to strengthen preventive measures," a move many are interpreting as a rejection of the Trump Administration's efforts to persuade the European Union (EU) to exclude Huawei from their still-to-be built 5G networks. The EC stated that "[t]he recommendations are a combination of legislative and policy instruments meant to protect our economies, societies and democratic systems…[and] [w]ith worldwide 5G revenues estimated at €225 billion in 2025, 5G is a key asset for Europe to compete in the global market and its cybersecurity is crucial for ensuring the strategic autonomy of the Union."

The EC recommended the following:

- Member States should complete their national risk assessments by **30 June 2019** and update necessary security measures. The national risk assessment should be transmitted to the Commission and European Agency for Cybersecurity by **15 July 2019**.
- In parallel, Member States and the Commission will start coordination work within the NIS Cooperation Group. Commission and the European Agency for Cybersecurity (ENISA) will complete a 5G threat landscape that will support Member States in the delivery by **1 October 2019** of the EU-wide risk assessment.
- By **31 December 2019**, the Network and Information Systems (NIS) Cooperation Group should agree on mitigating measures to address the cybersecurity risks identified at national and EU levels.
- Once the Cybersecurity Act, recently approved by the European Parliament, enters into force in the coming weeks, the Commission and ENISA will set up the EU-wide certification framework. Member States are encouraged to cooperate with the Commission and ENISA to prioritise a certification scheme covering 5G networks and equipment.
- By **1 October 2020**, Member States – in cooperation with the Commission – should assess the effects of the Recommendation in order to determine whether there is a need for further action. This assessment should take into account the outcome of the coordinated European risk assessment and of the effectiveness of the toolbox.

The Center for Strategic and International Studies' James Lewis wrote an article urging the Trump Administration to issue an "executive order (EO) on the security of telecom network supply chains and the use of suspect foreign technology." Lewis argued that U.S. allies and other countries may be far more inclined to banning Huawei than they will say in public, but they are holding back for a variety of reasons. One, they are unsure whether the U.S. push against Huawei is merely a part of the Trump Administration's larger push against China's trade practices. Consequently, a de facto U.S. ban could disappear in short order if China makes the right trade concessions. Also, there is fear of Chinese retaliation like when China stopped buying Australian coal after their ban was announced. Also, Huawei's prices are simply better than Nokia, Ericsson, and Samsung.

Lewis stated that "[i]deally, an EO would be part of a larger strategy for managing risk with the next generation of network technologies…[and] [t]he elements of a strategy should include:

1. Close partnerships with the countries that share the assessment of the risk of using Huawei and the need to act to address it.
2. Robust security standards for telecommunications equipment and supply chains (noting that some European customers of Huawei may try to dilute standards to ensure that Huawei has continued access to their markets).
3. Foreign assistance to encourage developing countries not to buy Huawei. We will not match Chinese subsidies, but we can reduce the financial burden of a ban.
4. Support for Western telecom infrastructure companies for research and development.
5. Research on how to securely communicate over international networks that contain Huawei equipment, since many African and Middle Eastern companies already use Huawei.
6. Formal bans (either complete or partial) on the purchase and use of Huawei technology.
7. An EO on telecom supply chain security that clearly lays out U.S. policy.
8. A long-term engagement strategy with China to bring its behavior into conformity with international norms for trade and security. China is not going away. It will always be powerful and the United States, working with its partners, must encourage and require change."

Quick Takes

"Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas." – *Washington Post*: "I believe we need new regulation in four areas: harmful content, election integrity, privacy and data portability:"

- "One idea is for third-party bodies to set standards governing the distribution of harmful content and to measure companies against those standards. Regulation could set baselines for what's prohibited and require companies to build systems for keeping harmful content to a bare minimum."
- "Online political advertising laws primarily focus on candidates and elections, rather than divisive political issues where we've seen more attempted interference. Some laws only apply during elections, although information campaigns are nonstop. And there are also important questions about how political campaigns use data and targeting. We believe legislation should be updated to reflect the reality of the threats and set standards for the whole industry."
- "I also believe a common global framework — rather than regulation that varies significantly by country and state — will ensure that the Internet does not get fractured, entrepreneurs can build products that serve everyone, and everyone gets the same protections. As lawmakers adopt new privacy regulations, I hope they can help answer some of the questions GDPR leaves open. We need clear rules on when information can be used

to serve the public interest and how it should apply to new technologies such as artificial intelligence."

- "Finally, regulation should guarantee the principle of data portability. If you share data with one service, you should be able to move it to another. This gives people choice and enables developers to innovate and compete."

"Manchin and King Press NERC on Electric Grid Reliability Efforts"– "Senators Joe Manchin (D-WV) and Angus King (I-ME) sent a letter to Mr. James Robb, Chief Executive Officer of the North American Electric Reliability Corporation (NERC) requesting information about NERC's efforts to protect the reliability of the United States' bulk power system from supply chain vulnerabilities, particularly those posed by vendors from Russia and China."
"[W]e request answers to the following questions:

1. Since August 2017, has NERC undertaken efforts to determine whether the bulk power system includes any components or software provided by Kaspersky, ZTE, or Huawei? If so, what were the results? If not, why not?
2. Has NERC issued guidance or recommendations to the users, owners, and operators of the bulk power system for mitigating the potential risks posed by components or software provided by Kaspersky, ZTE or Huawei?
3. What are NERC's next steps to mitigate the potential risks posed by components or software from Kaspersky, ZTE or Huawei?"

"FERC Staff Report Identifies Lessons Learned from CIP Reliability Audits" –"Federal Energy Regulatory Commission (FERC) staff today issued a report offering recommendations to help users, owners and operators of the bulk-power system assess their risks, compliance efforts and overall cyber security posture." Among the report's recommendations:

- Consider implementing valid Security Certificates within the boundaries of BES Cyber Systems with encryption sufficiently strong enough to ensure proper authentication of internal connections;
- Consider implementing encryption for Interactive Remote Access that is sufficiently strong enough to protect the data sent between the remote access client and the BES Cyber System's Intermediate System; and
- Consider replacing or upgrading "End-of-Life" system components of an applicable Cyber Asset."

Other Hearings and Events

"Implementing the 21st Century Cures Act: Making Electronic Health Information Available to Patients and Providers" – Senate Health, Education, Labor, and Pensions

Further Reading

"This Spyware Data Leak Is So Bad We Can't Even Tell You About It" – *Motherboard*
"CEO of Israeli spyware-maker NSO on fighting terror, Khashoggi murder, and Saudi Arabia" – *60 Minutes*
"After Mueller, a more public-spirited president would join Congress to defend the 2020 election" – *Washington Post*
"Insurers Creating a Consumer Ratings Service for Cybersecurity Industry" – *The Wall Street Journal*
"Industry groups urge state legislators to oppose tracking software bills" – *statescoop*
"How Las Vegas Stops Email-Borne Cyberattacks Pre-Delivery" – *Nextgov*

"Chinese-speaking phone scammers stole $40 million, mostly from Chinese targets in the U.S., FBI says" – *cyberscoop*
"'58 Million Names And Addresses, Please' - Tech Giants Reveal Wild Government Requests for Data" – *Forbes*
"Told U.S. security at risk, Chinese firm seeks to sell Grindr dating app" – *Reuters*