Technology Policy Update
7 November 2019
By Michael Kans, Esq.

A Privacy Bill A Week: the Obama Administration's "Consumer Privacy Bill of Rights Act of 2015"

Last week, we took a look at two bills that approach privacy issues from the vantage of data ownership: Senator John Kennedy's (R-LA) "Own Your Own Data Act" (S. 806), and Senators Mark Warner (D-VA) and Josh Hawley's (R-MO) "Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data" (S. 1951). This week, we are going to be time-traveling, in a way, as we will look at the last bill put forth by a White House on privacy, the discussion draft of the "Consumer Privacy Bill of Rights Act of 2015" released by the Obama Administration. This bill was released in conjunction with a report on privacy issues and then proceeded to go nowhere as there was scant appetite on Capitol Hill to legislate on privacy. Nonetheless, this bill is fairly comprehensive and contains a number of concepts that are present in the most recent bills.

The bill has a very broad definition of "personal data," at least as broad as some of the more consumer-friendly bills, but it has a safe harbor for de-identified information, which would not be considered "personal data" for purposes of the act. To wit, "personal data" are "any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual." The bill provides examples of what might be personal data but makes clear that the enumerated examples are not the only possible information that will be covered under the bill. Aside from the usual types of data named in privacy bills, a few bear mention. First "biometric identifiers" are considered "personal data" such as fingerprints or voice prints, but not biometric data more generally. Additionally, genetic data are not identified either. However, the base definition of personal data is so broad, it would be a hard argument to make that biometric and genetic data, much of which is easily linkable to individuals or devices and not generally made available to the public, do not qualify. Besides, the definition itself does state that the examples "include" but are "not limited to" those specifically spelled out.

However, like a number of the other bills, the "Consumer Privacy Bill of Rights Act of 2015" provides detailed exceptions to what might other be "personal data." Consequently, de-identified, deleted, and cybersecurity data are not personal data subject to the requirements of the bill. Regarding de-identified data, a covered entity would need to render the data such that it could reasonably be expected to be identified once to a person or device. Presumably encryption would suffice so long as the encryption keys are not compromised, and other processes such as anonymization would qualify. However, such covered entities must commit publicly to not try to re-identify such data and put in place processes to execute this promise. Moreover, any third party with whom the covered entity shares the de-identified data must also make the same public commitment not to re-identify such data. The definition of "deleted data" is pretty straightforward and squares with the common understanding of what deleting is.

That the bill singles out "cybersecurity data" dates the bill. As many might recall, this was the point during the Obama Administration when the there was a push to enact cybersecurity information

sharing legislation that ultimately culminated in Title I of the "Cybersecurity Sharing Act of 2015" (Division N of P.L. 114-113). Consequently, this definition is tailor-made for the new procedures that bill set up: "cyber threat indicators collected, processed, created, used, retained, or disclosed in order to investigate, mitigate, or otherwise respond to a cybersecurity threat or incident, when processed for those purposes." Not surprisingly, "cyber threat indicator" is also defined, and the salient part of the legislation is that for any such information, there must be "reasonable efforts…to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat." And, employee data is also excepted, but this definition is tightly written and would pertain to only the types of and uses for which employment information has usually been used, and any information uses beyond these would possibly then become "personal data" subject to enforcement. Also of note, this definition *does not* include the personal data of job applicants, but those data are excluded for small businesses in the definition of a covered enity.

Those entities covered by the new privacy regime are any person "that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce" subject to exceptions, namely:

- federal, state, and local governments, including any contractors and agents working on their behalf;
- any "natural person" acting in a "de minimis" capacity in collecting and processing personal data;
- Any entity with 25 or less employees would not be covered based on the data processing it does of applicant's personal data "in the ordinary course"
- Any other entity, or class of entities, the FTC identifies through a rulemaking; and
- Those entities using personal data "to conduct research relating directly to security threats to or vulnerabilities in devices or networks, or to address threats or vulnerabilities identified by that research" subject to additional security and disclosure requirements

The "covered entity" exception list includes a more detailed, complicated exception: an entity with 5 or fewer employees that "collects, creates, processes, uses, retains, or discloses" the personal data of less than 10,000 people during any 12-month period might also be excepted. However, such entity may not "knowingly collect, use, retain, or disclose any information that is linked with personal data and includes, or relates directly to

- that individual's medical history;
- national origin;
- sexual orientation;
- gender identity;
- religious beliefs or affiliation;
- income, assets, or liabilities;
- precise geolocation information;
- unique biometric data; or
- Social Security number.

However, any entities that "knowingly collect, use, retain, or disclose" this information *would be* covered only regarding this information and would need to comply with the bill. And yet, excluded from that list of activities is processing, suggesting that the knowing processing of those personal data would *not be* excepted and would be also covered by the requirements of the bill regardless of the size of the entity.

The bill provides that "[e]ach covered entity shall provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous notice about the covered entity's privacy and security practices." However, notice must be "reasonable in light of context," and the bill defines what "context" which are "circumstances surrounding a covered entity's processing of personal data," including a number of enumerated considerations such as the "extent and frequency" of interaction, the history between consumers and the covered entity, a reasonable person's understanding of how the covered entity processes and uses data in providing services and products

Among other information covered entities would need to provide include:

- The personal data processed, including data acquired from other sources
- The purposes of its data processing
- The people, or categories of people, to whom data is disclosed and the purposes to which such data may be used
- When personal data may be deleted, destroyed, or de-identified
- How consumers may "access their personal data and grant, refuse, or revoke consent for the processing of personal data"
- How personal data is secured; and
- To whom may a consumer complain or inquire regarding the covered entity's data processing practices

In terms of the protections people would get under the "Consumer Privacy Bill of Rights of 2015," "[e]ach covered entity shall provide individuals with reasonable means to control the processing of personal data about them in proportion to the privacy risk to the individual and consistent with context." This sounds like strong language that would shift the balance in the user-company data relationship, but there appears to be an inherent balancing of interests in this right such that a person's control of data processing would be proportional to privacy risks and appropriate for the context.

Nonetheless, covered entities must provide easy to find, use, access, and understand controls for people. Additionally, people must be able to withdraw their consent in similarly easy fashion, so covered entities would also need to offer this option to users. What's more, covered entities must delete the personal data of any user that withdraws consent no later than 45 days after such a withdrawal is made. Of course, should a user indicate she wants to withdraw consent, a covered entity may offer her the option that the company still hold the data but de-identify it. The bill is silent on whether the covered entity would ever be able to re-identify the data without the consent of the user, however. Likewise, it is also not clear whether "alternative means of compliance" can wholly replace the requirement that a person's data be deleted in the event he withdraws consent. If a covered entity can offer only de-identification instead of deletion in the event a consumer withdraws consent, it's my guess that most entities would do so in the hopes of one day reobtaining the person's consent.

There is also a curiously constructed limitation of the covered entity's obligations regarding the right to withdraw consent. This right pertains only to the data the covered entity has in its control, and hence does not cover personal data the entity may have collected and then shared with other entities. Does this mean consumers intent on ensuring their withdrawal is effective across entities would need to somehow determine which entities are holding their personal data? It appears so. Putting that issue aside, the withdrawal and subsequent deletion or de-identification does not apply to "enumerated exceptions," a term defined in the bill as including:

- Preventing or detecting fraud, child exploitation, or serious violent crime
- Protecting device, network or facility security
- Protecting a covered entity's rights or property or those of an entity's consumer if consent has been given
- Monitoring and enforcing agreements, including terms of service
- "Processing customary business records"
- "Complying with a legal requirement or an authorized government request"

So, any such information would not need to be deleted or de-identified in response to a withdrawal of consent.

The latter two exceptions are quoted directly since they seem to present the most latitude. "Customary business records" is defined in the bill as "data, including personal data, typically collected in the ordinary course of conducting business and that is retained for generally accepted purposes for that business, including accounting, auditing, tax, fraud prevention, warranty fulfillment, billing, or other customary business purposes." Therefore, it would hard going to try to shoehorn into this definition the collection and processing of personal data by a data broker or company conducting similar operations. The last exception seems a bit more elastic, however. Complying with. Legal requirement would seem to cover all federal, state, and local legal requirements that are not otherwise contrary to the preemption language in the bill. However, an "authorized government request" would seem to run the gamut from an administrative subpoena to a warrant. Of course, under the Electronics Communications Privacy Act (ECPA), the type of provider determines the threshold a law enforcement agency needs to clear to access stored communications. Furthermore, this definition of "enumerated exceptions" is used throughout the bill to carve out these activities from those that may be regulated by the FTC.

Returning to the withdrawal of consent, covered entities may also offer an alternative to deletion such they would instead offer to de-identify personal data. And yet, it is not clear whether the covered entity is complying by only presenting the option to de-identify instead of delete. Of course, the definition of de-identified data entails a public commitment not to re-identify and this obligation travels with the de-identified data such that any third parties to whom such data is disclosed would then need to honor it. Presumably, violations of this commitment are grounds for FTC action. However, it may be contrary to the larger goals of the bill and the public interest to allow companies to sit on troves of de-identified data that may well prove easy enough to re-identify after being exfiltrated or accessed. Finally, users must be given advance notice of material changes to the collection, use, or sharing practices of a covered entity and also a mechanism to control the resulting privacy risk.

Turning to the section titled "Respect for Context," it is established that any covered entity processing personal data "in a manner that is reasonable in light of context" is not subject to the extensive requirements in this section of the bill. Two definitions bear scrutiny if this exception is to make sense. First, "process[ing] personal data" is "any action regarding data that is linked to an individual or a specific device, including but not limited to collecting, retaining, disclosing, using, merging, linking, and combining data." I would wonder if the processing of personal data that is *linkable* to a person or device would qualify, and if not, this would seem to be a significant loophole. The other definition worthy of a look is "context," which is detailed and lengthy, but most succinctly, it "means the circumstances surrounding a covered entity's processing of personal data," which may include the history and frequency of direct actions between an individual and a covered entity,

However, the enumerated circumstance that can constitute "context" that is among the more flexible is "the level of understanding that reasonable users of the covered entity's goods or services would have of how the covered entity processes the personal data that it collects, including through any notice provided by the covered entity." This construct employs the reasonable person construct from Tort law to set a baseline. More significantly, if a covered entity provides easily understood notice that is easily accessible that a reasonable person can understand regarding the covered entity's data processing, then it would appear there would not be much off-limits.

However, any data processing that is not reasonable in the context would trigger additional responsibilities for covered entities to conduct a privacy risk analysis to examine possible privacy risks and steps to mitigate these risks. Additionally, a covered entity must provide notice of any data processing that is unreasonable in light of context and provide a mechanism that allows for a reduction in risk exposure. This section would allow an exception for "data analysis" supervised by a Privacy Review Board," a type of entity that would be permitted under FTC regulations, based on a range of factors. It bears note that "data analysis" is a new concept in this legislation and appears to be a subset of data processing; however, it is not entirely clear what is encompassed by data analysis. Nonetheless, any personal data analysis that is unreasonable in light of the context that results in adverse action against multiple individuals triggers a requirement that a covered entity conducts a disparate impact analysis according to accepted standards that it must keep on file.

The "Consumer Privacy Bill of Rights" established a process for a new class of entities, Privacy Review Boards, that would need to apply to and be certified by the FTC before they could operate to supervise the data analysis of covered entities.

Covered entities may only collect, retain, and use personal data that is reasonable in light of the context and must consider ways and means to minimize privacy risks. However, it is unclear if any such identified means of reducing privacy risks must actually be implemented. Additionally, any such personal data must be destroyed, deleted, or de-identified after a reasonable period of time following the purposes for which the data was collected has been achieved. But, there are exceptions to these two general requirements, including the "enumerated exceptions" discussed before, data analysis performed under Privacy Review Board supervision, and under the heightened notice and control procedures discussed earlier for data processing unreasonable in light of the context.

Covered entities would need to establish and maintain security and privacy programs to guard against unauthorized access disclosure, misuse, alternation, destruction, or compromise of personal data. Such programs would start with risk assessments to suss out weaknesses and vulnerabilities that the subsequent security and privacy programs would ideally remedy with an eye towards addressing foreseeable risks as well. This section of the bill spelals out the sort of considerations covered entities should be heeding and quite likely the approach the FTC would take in policing security and privacy violations:

- The privacy risks posed by the personal data being held, for not all data are equally valuable
- The foreseeability of threats
- Widely accepted and used administrative, technical, and physical safeguards; and
- The costs associated with implementing security and privacy safeguards.

This approach to spurring entities to implement security and privacy programs is familiar and has been the general approach since at least the safeguards rules promulgated per the "Financial Modernization Act of 1999" (Gramm-Leach-Bliley).

Covered entities will also need to provide each individual access to her personal data in a reasonable timeframe if such a request is made subject to verifying the requester's identity, relevant laws and regulations, the degree to which the request is vexatious or frivolous, and whether a fraud investigation or national security, intelligence, or law enforcement purpose presents a compelling reason to deny access. What's more, there is a duty to ensure that such information is accurate and individuals will have a means to dispute or amend inaccurate personal data held by a covered entity. And yet, if the personal data subject to a request to correct or amend would not likely result in adverse action against an individual, the covered entity may decline the request. However, an individual may further request that these data be deleted and or destroyed, and covered entities would need to comply with 45 days with the personal data from government records being excepted.

Each covered entity must take appropriate measures consistent with the privacy risks connected to its personal data processing practices, including:

- Train staff who handles these data
- Executing both internal and independent audits and evaluations for privacy and security
- Building privacy and security into systems
- Binding third parties with whom personal data are shared with the obligation to meet the same responsibilities incumbent on covered parties.

The "Consumer Privacy Bill of Rights" makes any violations as being contrary to Section 5 of the FTC Act, which bars unfair and deceptive practices. The FTC would receive authority to levy civil fines in some circumstances and its jurisdiction widened to include non-profits under the bill. The FTC could seek fines for first offenses committed knowingly or with constructive knowledge of up to $35,000 per day of violations, and not like other bills, on a per victim basis. However, if the FTC puts a covered entity on notice with particularity as to the ways it is violating the bill, then the FTC could seek per victim fines of $5,000 per person. In any event, civil penalties are capped at $25 million. State attorneys general would also be allowed to enforce the act, in part, and in acting without the FTC may only seek injunctive relief and not civil fines. And yet, there is no private right of action for individuals.

The bill would allow for the development of codes of conduct for processing personal data that covered entities could abide by in exchange for liability protection. These codes would need to provide an equal or greater level of protection for processing than the underlying statute. Within six months of enactment, the FTC would need to establish the regulations spelling out the process by which entities may craft and submit such codes of conduct. The FTC would examine whether the code provides an equal or greater level of protection for processing than the statute itself and resulting regulations. Any codes developed through a transparent, multi-lateral process led by the Department of Commerce must be approved or denied within 90 days, any transparent and multi-lateral process to develop a code led by another entity within 120 days, and all others within 180 days. However, these codes must be published for public comment before the FTC rules on them. If approved, a code must be reviewed every 3-5 years to determine how it has worked and whether it is still viable given technological and societal changes and possibly extended.

Additionally, entities may apply to the FTC to administer a code of conduct for the processing of personal data once it's been approved, and such certification may be granted if the entity can prove it can expeditiously and efficiently adjudicate violations. All such certifications will be reviewed by the FTC within 3-4 years of being granted and possibly renewed.

Covered entities that publicly commit to a code of conduct that adhere to the code may assert it as a complete defense to an enforcement action brought by the FTC or a state attorneys general, and any claims regarding the data processing the code covers might be null and void. And, it is wise to revisit the definition of processing personal data which "means taking any action regarding data that is linked to an individual or a specific device, including but not limited to collecting, retaining, disclosing, using, merging, linking, and combining data." Consequently, a code could provide quite a bit of liability protection provided on how it is drafted and what it covers, of course.

Regarding preemption, the bill would preempt all conflicting state or local laws "to the extent" one "imposes requirements on covered entities with respect to personal data processing," but then also stipulates that "[n]o State or local government may enforce any personal data processing law against a covered entity to the extent that that entity is entitled to safe harbor protection" under a code of conduct." But if such laws are already preempted, how could states or localities enforce one? Perhaps, this passage is intended to ward off attempts by states or local governments to use consumer protection statutes, which are expressly not preempted, to try to get around the preemption of their data processing laws. Moreover, other state causes of action remain untouched such as those under contract, tort, trespass, fraud, and others, meaning that covered entities would stull possibly face such actions. The "Consumer Privacy Bill of Rights Act" also would impinge First Amendment rights and any activities under Section 230 would also be exempted. Finally, the bill does not modify, alter, or supersede the operation of any federal privacy or security statute (e.g. HIPAA) in governing the conduct of an otherwise covered entity. But, this goes only as far as the four corners of the other statute, and all conduct outside that statute regarding data processing would seem to fall into the FTC's jurisdiction to enforce this Act unless the agency lacks jurisdiction over that class of entities (e.g. banks and credit unions.)

Hearing on 5G and National Security

The Senate Homeland Security and Governmental Affairs Committee held the latest in a series of hearings across the many committees of jurisdiction regarding the national security and economic issues posed by the coming rollout of fifth generation (5G) networks, particularly in light of Huawei's seemingly insurmountable dominance in this market. Some of the previous hearings include:

- In February, the Senate Commerce, Science, and Transportation Committee examined "winning" the 5G "race"
- In May, the Senate Judiciary Committee looked at the interplay between national security and intellectual property
- In late September, the House Energy & Commerce Committee delved into 5G

In October 2018, President Donald Trump released his "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," that asserted

> it is imperative that America be first in fifth-generation (5G) wireless technologies — wireless technologies capable of meeting the high-capacity, low-latency, and high-speed requirements that can unleash innovation broadly across diverse sectors of the economy and the public sector. Flexible, predictable spectrum access by the United States Government

> will help ensure that Federal users can meet current and future mission requirements for a broad range of both communications- and non-communications-based systems.

This memorandum then detailed the various actions agencies must take to implement the strategy. And, while the National Telecommunications and Information Administration (NTIA) was tasked with developing a "National Spectrum Strategy" and asked for comments in late 2018, the agency has not yet released this strategy." However, the White House's Office of Science and Technology Policy (OSTP) released the results of its collaboration with the Wireless Spectrum R&D (WSRD) Interagency Working Group, released a report "Research and Development Priorities for American Leadership in Wireless Communications." OSTP also released its report on "Emerging Technologies and their Expected Impact on Non-Federal Spectrum Demand." The White House claimed that "[t]hese reports will inform the National Spectrum Strategy and ensure American leadership in terrestrial wireless and satellite technologies for 5G and beyond."

Chair Ron Johnson (R-WI) stated that "[w]e are at a technological crossroads." He stated that "[w]hile the development of 4G wireless technology made innovations like Uber and Netflix possible, the transition to 5G promises connectivity that is 100 times faster and five times more reliable." Johnson claimed that "[i]t will also enable us to connect exponentially more devices at the same time, a capability that will empower the Internet of Things, which will inter-connect all modern devices, as well as innovations like artificial intelligence and smart cities." He contended that "this progress is not inevitable."

Johnson stated that "[a]ccording to FBI Director Christopher Wray, the vulnerabilities associated with the development and deployment of 5G technology, especially the threat posed by China, is one of the 'generational threats that will shape our nation's future.'" He claimed that "threat relates both to national and economic security…[and] [w]hen it comes to cyber attacks and cyber espionage, China is a known bad actor." He noted that "China was responsible for the 2015 Office of Personnel Management (OPM) data breach and is suspected to be behind other high-profile security breaches, like the Anthem and Marriott breaches." Johnson claimed that "[w]hether highly-sensitive and classified national security information or the private information of American consumers, China will do whatever it can to steal information from competitors." He claimed that "[r]ecognizing China's intent and its domestic laws requiring its companies to do whatever is asked of them, there is serious cause for concern with having a Chinese-backed telecommunications company responsible for major components of 5G networks."

Johnson stated that "[w]ith regard to our economic security, winning the race to 5G is worth billions of dollars for the U.S. economy…[and] [i]t is imperative that the U.S. maintain its global leadership with 5G and not let adversaries like China and other competitors seize the first-mover's advantage, which includes setting the standards for a host of related technologies, and the related economic benefits." Johnson asked "[h]ow are we, as a nation, planning to address the threat posed by China and ensure we win the race to 5G?" He asserted that "[a]t the outset, it is imperative to recognize that the federal government cannot do this alone…[and] [a]lthough recent legislation and an executive order include efforts to secure the federal government against threats posed by Chinese information communications technology, or ICT, companies, the vast majority of this risk rests with the private sector and state or local governments." Johnson claimed that "[t]he federal government must work in coordination with private sector experts to ensure that we have the processes, authorities, and resources necessary to address the challenges inherent in this effort."

Johnson argued that "[t]hese challenges are not restricted to the homeland…[and] [e]ven as the U.S. works to secure its own infrastructure, our increasingly interconnected world means that the U.S. is also at risk from the vulnerabilities in the wireless networks of other countries." He contended that "[a]ny country whose information and communication technology (ICT) supply chains run through China, a nation that uses cyber espionage as a way of doing business, is at grave risk." He contended that "[t]hus, because of the nature of the problem, any true solution must be comprehensive, which requires the U.S. to act in concert with its international allies and partners." Johnson declared that "[t]he U.S. must also confront the reality that some allies and partners will not or cannot avoid entirely the use of Chinese ICT from essential parts of their 5G networks" and asked "[w]hat should we do in those instances?"

Johnson stated that "[t]his is an extraordinarily complicated task, but to make matters more challenging, I am not convinced that we have a consensus between the various federal government agencies on what the problem is that we are trying to tackle." He claimed that "access to the most sound and creative thinking means little without the ability to transform it into action…[and] [t]o do that, we must be able to answer foundational questions: Who's in charge of guiding these complex conversations and making the tough decisions? Who will define what "success" on 5G looks like from a national security perspective?" Johnson remarked that "[g]enerational problems cannot be solved without a shared understanding of the problem and an agreed-upon approach for addressing it."

Ranking Member Gary Peters (D-MI) stated that "[t]he introduction of 4G technology brought us live-streaming, ridesharing, on-demand delivery, and other innovations…[a]nd now, the 5G era is at hand." He claimed that "[t]his faster, stronger wireless connection will once again transform our digital world, enabling new technologies like precision agriculture, self-driving cars, and augmented reality." Peters stated that "5G networks and the new technologies they spur will create countless new jobs in Michigan and generate billions of dollars in economic growth across our country." He said that "5G has the potential to unleash new productivity and help cement the United States as a global leader in innovation…[b]ut developing the infrastructure needed to support 5G networks across the country does not come without risks."

Peters stated that "[t]oday, China, arguably our nation's greatest global competitor, is poised to lead the world in advancing this important technology." He claimed that "China's edge in the development of 5G equipment and standards poses a threat to both American economic dominance and to our national security…[and] [t]he U.S. is increasingly reliant on high-speed telecommunications services to support not only our broader economy, but also our entire defense industry." Peters stated that "[i]n the race to expand 5G access, we face serious supply chain security risks by purchasing and deploying Chinese-made equipment from companies like Huawei and ZTE, companies our Intelligence Community has said may be beholden to the Chinese government." He stated that "[t]he devices these companies provide potentially offer cost-effective solutions to help close the digital divide…[b]ut they also pose a serious national security risk and could open a backdoor into critical American security networks."

Peters said that "[g]iven these serious national security risks, we must navigate a delicate balance of ensuring that emerging 5G networks are both secure and widely available in rural and urban areas…[and] China's advantage in 5G may be a reality for now." He asserted that "it is also something that we have the power to change." Peters said that "[t]he United States government, including this Committee, has an opportunity to play a key role in America's resurgence as a leader in the development of 5G networks." He stated that "[a] challenge of this magnitude requires a

strong, unified and collaborative approach – capitalizing on the full power of American ingenuity." Peters claimed "[b]ut to date, our efforts have been piecemeal and disorganized…[and] [w]e do not have the dedicated leadership or the coordinated national strategy needed to accomplish this critical mission." He said that "I am encouraged by the bipartisan agreement this Committee has made to support this goal." Peters said that "[u]niversal 5G connectivity would encourage renewed prosperity in both urban and rural communities, unlock tremendous economic growth, and reestablish America as a leader in global innovation."

Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs stated that "[t]o manage and address the risks posed by 5G, the U.S. government is taking an interagency approach to this issue, led by the White House." He said that the "National Security Council (NSC) Cybersecurity Directorate and the National Economic Council co-lead a regular 5G interagency Policy Coordination Committee (PCC) through the National Security Presidential Memoranda (NSPM) -4 process." Krebs stated that "[t]hese meetings are an opportunity to discuss and come to decisions on key 5G issues, such as participation in standards bodies, as well as to provide updates on interagency 5G activities."

Krebs stated that "[r]educing ICT supply chain risk is a national security imperative and one that is a key pillar of CISA's Strategic Intent…[and] [w]hile many components of CISA play some role in supporting supply chain initiatives, the National Risk Management Center (NRMC) leads the agency-wide supply chain coordination effort –providing program management and analytical support to current lines of effort…[and] [t]hese include:

- The ICT Supply Chain Risk Management Task Force
- ICT analysis in support of Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain
- 5G mobile communications security and resilience efforts

Krebs stated that

> From my perspective, 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years and, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today to secure tomorrow. 5G builds upon existing telecommunication infrastructure by improving the bandwidth, capacity, and reliability of wireless broadband services. The evolution will take years, but the goal is to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the Internet of Things (IoT), ultra-low latency required for critical near-real time data transmission, and faster speeds to support emerging technologies. As of June 2019, 5G networks and technologies are in development with a limited rollout in select cities around the world, including 20 in the United States. The Department of Homeland Security (DHS), working with its interagency and industry partners, has an opportunity to help shape the rollout of this emerging critical infrastructure, increasing its security and resilience at the design phase and reducing national security risk from an untrustworthy 5G network. Our intent in doing so is to promote the development and deployment of a secure and resilient 5G infrastructure that enables enhanced national security, technological innovation, and economic opportunity for the United States and its allied partners. Our work in this area will be focused on six lines of effort, to include:
>
> - Support the design and deployment of 5G networks with security and resilience in mind, to include investing in Research & Development
> - Promote 5G use cases that are secure and trustworthy

- Identify and communicate risks –including supply chain risks –to 5G infrastructure
- Promote development and deployment of trusted 5G components
- Advance the United States' global effort to influence direction of allied nations in 5G deployments
- Provide leadership role within USG to coordinate operational 5G security and resilience efforts

Deputy Assistant Secretary of State for Cyber and International Communications and Information Policy Robert Strayer said that "[t]he Department of State, under Secretary Pompeo's leadership, is in charge of the United States' international engagement on ICT security and our campaign to convince our allies and partners of the importance of 5G security." Strayer stated that "[a]s countries around the world upgrade their communications systems to 5G technology, we are urging them to adopt a risk-based security framework." He said that "[t]o this end, the Department is executing a global campaign on 5G security that includes strategic bilateral and multilateral engagements to convince our allies and partners of the importance of adequately securing these networks." Strayer asserted that "[a]n important element of this risk-based security approach is a careful evaluation of hardware and software equipment vendors and the supply chain…[and] [t]he evaluation criteria should include the extent to which vendors are subject to control by a foreign government with no meaningful checks and balances on its power to compel cooperation of these vendors with its intelligence and security agencies."

Strayer stated that "[w]hile this should apply to vendors from all countries, our current concern is primarily with equipment vendors from the People's Republic of China (PRC) for multiple reasons." He said that "[o]ur assessment of the problem is that the PRC could compel Chinese equipment vendors to act against the interests of U.S. citizens and citizens of other countries around the world." Strayer said that "[i]f allowed to construct and service 5G networks, Chinese equipment vendors will have access to critical networks and understanding of network vulnerabilities." Strayer claimed that "[t]his information could be exploited, as outlined in China's National Intelligence Law, for the Chinese Communist Party to disrupt critical infrastructure, intercept sensitive transmissions, and acquire sensitive technology and intellectual property."

Strayer stated that "the European Commission and member states released their coordinated risk assessment of 5G security…[and] [w]e welcomed the assessment and how it clearly identified the vulnerability of 5G vendors or suppliers that could be subject to pressure or control by a third country, especially countries without legislative or democratic checks and balances in place." He contended that "[t]he assessment also highlighted the corporate ownership structure of 5G suppliers as a potential risk factor, which aligns with the U.S. assessment and the Prague Proposals' call for transparency."

Strayer stated that "[i]n addition, the assessment recognized that the "edge" and "core" of networks will blur in 5G networks, requiring increased security measures be applied to all parts of the network." He claimed that "[t]his aligns with the U.S. assessment that you cannot mitigate the risk of untrusted suppliers by limiting them to certain parts of a network…[and] [u]ntrusted suppliers anywhere in the network could be exploited by authoritarian governments for espionage, traffic disruption, data manipulation, and/or theft of sensitive information and intellectual property."

Strayer stated that "[t]he EU risk assessment itself is a sign of progress in our 5G campaign as it demonstrates that our allies and partners are recognizing the risk of untrusted vendors, but our work is far from over." He explained that "[n]ext, the European Commission and member states will use

this assessment to develop and agree upon "a toolbox of possible risk mitigating measures" by the end of the year." Strayer stated that "[t]his toolbox will outline specific, albeit non-binding, actions that member states can take to secure their 5G networks…[and] [i]t is important that this toolbox address the vulnerabilities and risks identified in the EU's risk assessment, including from untrusted suppliers, and that member states then implement binding national measures to safeguard their networks."

Federal Communications Commission (FCC) Commissioner Jessica Rosenworcel stated that "[f]or the last decade, the United States has led the world in wireless technology and performance, and we have reaped the benefits." She declared "[t]hat authority is now being challenged." Rosenworcel stated that "[e]xtending this leadership into the next generation of wireless technologies—5G—is going to be difficult…[b]ut it's worth the effort." She stated that "[w]ith speeds as much as 100 times faster than present networks and much lower latency, these networks will kickstart the next big digital transformation." Rosenworcel noted that "earlier this year the Defense Innovation Board—the United States military's premier advisory board of academic researchers and private sector technologists—surveyed the state of next-generation 5G networks and issued a sober warning." She said that "[t]hey found that 'the country that owns 5G will own innovations and set the standards for the rest of the world,' and 'that country is currently not likely to be the United States.'" Rosenworcel stated that "[t]his is a clarion call…[for] [o]ther nations saw very clearly the success in the United States with the last generation of wireless technology and are working overtime to ensure that they secure a leadership position—and their efforts are bearing fruit."

Rosenworcel stated that "[t]he truth is we are facing well-resourced challenges to our 5G leadership from every direction…[a]nd so far, we do not have a comprehensive national plan in place with a fully coordinated interagency response to meet that challenge." She asserted that "[w]e need one—and here are four ideas it should include:

- First, if we want to lead in 5G, we have to secure the 5G supply chain. The underlying truth about next-generation communications networks in many parts of the world is that technology developed in China will be at the center. This threatens to expose our networks and our most private data to undue foreign influence. The good news is we are making some progress with our federal networks.
- Second, we need an approach to supply chain security that recognizes that despite our best efforts, secure networks in the United States will only get us so far because no network stands by itself. Our networks still will connect to insecure equipment abroad. So we need to start researching how we can build networks that can withstand connection to equipment vulnerabilities around the world. One way to do this is to invest in virtualizing radio access networks—or open RAN. The RAN is the most expensive and restrictive part of the network—it sits between your device and a carrier's core network. Today, all major components of a RAN have to come from the same vendor. There is no way to mix and match. But if we can unlock the RAN and diversify the equipment in this part of our networks, we can increase security and push the market for equipment to where the United States is strongest—in software and semiconductors. This also will give carriers around the world that are locked into upgrade cycles with a single foreign vendor a way out.
- Third, we need smarter spectrum policy. To date, the FCC has aggressively focused its early efforts to support 5G wireless service by bringing only high-band spectrum to market. This is a mistake. The rest of the world does not have this singular early focus on high-band, millimeter airwaves, with good reason. These airwaves have substantial capacity but their signals do not travel far and are easily blocked by walls. As a result, commercializing them is costly—especially in rural areas. The sheer volume of antenna facilities required to make

this service viable will limit deployment to the most populated urban areas. This means our early 5G spectrum policy could create 5G haves and have-nots, deepening the digital divide that already plagues too many rural communities nationwide. That's not right. If you care about rural broadband, this matters. The FCC needs to change course and make it a priority to auction mid-band spectrum, which has a mix of capacity and propagation which is better suited to extend the promise of 5G wireless service to everyone, everywhere in the country.

- Fourth and finally, with 5G we are moving to a world with billions of connected devices around us in the internet of things. We need to adjust our policies now to ensure this future is secure. After all, the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks. Here is what that could look like. Every device that emits radiofrequency at some point passes through the FCC. If you want proof, pull out your smartphone or take a look at the back of any computer or television. You'll see an identification number from the FCC. It's a stamp of approval. It means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States. This routine authorization process takes place behind the scenes. But the FCC needs to revisit this process and explore how it can be used to encourage device manufacturers to build security into new products.

FTC Acts Against Deceptive Online Advertising

The Federal Trade Commission (FTC) took action in two cases of deceptive online advertising, one against a company selling social media influence and the other against a company for posting fake reviews of its products on a third party's site.

In its complaint against Devumi, the FTC asserted that "the Devumi.com, TwitterBoost.co., Buyview.co, and Buyplays.co websites…sold fake indicators of social media influence, including fake followers, subscribers, views, and likes, to users of different social media platforms, including LinkedIn, Twitter, YouTube, Pinterest, Vine, and SoundCloud." For these practices, the FTC made the case that Devumi and the other companies engaged in unfair and deceptive practices in violation of Section 5 of the FTC Act. The FTC claimed that these companies "have provided such users of social media platforms with the means and instrumentalities for the commission of deceptive acts or practices" by allowing paying customers to gain users or views across a range of social media platforms. In the proposed order entered in the U.S. District Court for the District of Southern Florida, the FTC permanently barred the defendants from selling or misrepresenting social media influence. Additionally, the settlement calls for a $2.5 million in equitable monetary relief, which shall be suspended so long as the CEO of the company personally responsible pays his $250,000 fine.

The FTC also announced its proposed administrative action against Sunday Riley and its namesake CEO for posting fake reviews of its cosmetic products on the website of retailer Sephora. Sunday Riley executives and employees created fake accounts to post fake reviews, and then used a VPN once the reviews were taken down. CEO Sunday Riley also directed employees to create three different fake accounts for this purpose. The FTC is proposing to bar Sunday Riley and the named parties from making any misrepresentations against the company's products.

In their statement explaining their no vote, Commissioners Rohit Chopra and Rebecca Kelly Slaughter asserted that the "proposed settlement includes no redress, no disgorgement of ill-gotten gains, no notice to consumers, and no admission of wrongdoing." They argued "the proposed settlement is unlikely to deter other would-be wrongdoers." Chopra and Slaughter Kelly added:

> Consider the cost-benefit analysis that a firm might undertake in considering whether to engage in review fraud. The potential benefits are substantial: higher ratings, more buzz, better positioning relative to competitors, and higher sales. The direct costs of generating reviews are minimal, certainly far less expensive than traditional advertising. The biggest potential cost is if the wrongdoer is caught, but it is likely that the vast majority of fake review fraud goes undetected. Even fake reviews that are detected may simply be removed with no sanction against the creator.

Chopra and Kelly Slaughter stated that "[t]he proposed resolution of this matter suggests that even the narrow subset of wrongdoers who are caught and attract law enforcement scrutiny will face minimal sanctions."

ACCC Charges Google With Violations Of Consumer Laws Over Android Location Settings

The Australian Competition and Consumer Commission (ACCC) announced a legal action against Google "alleging they engaged in misleading conduct and made false or misleading representations to consumers about the personal location data Google collects, keeps and uses" according to the agency's press release. In its initial filing, the ACCC is claiming that Google mislead and deceived the public in contravention of the Australian Competition Law and Android users were harmed because those that switched off Location Services were unaware that their location information was still be collected and used by Google for it was not readily apparent that Web & App Activity also needed to be switched off. ACCC Chair Rod Sims explained that "[w]e are taking court action against Google because we allege that as a result of these on-screen representations, Google has collected, kept and used highly sensitive and valuable personal information about consumers' location without them making an informed choice." Moreover, it is being reported in the Australian press that the ACCC is preparing an anti-competitive action against Google based on its actions against an Australian competitor, Unlockd, that subsequently filed for administration last year.

In its press release, the ACCC claimed

> [T]hat from at least January 2017, Google breached the Australian Consumer Law when it made on-screen representations on Android mobile phones and tablets that the ACCC alleges misled consumers about the location data Google collected or used when certain Google Account settings were enabled or disabled. The representations were made to consumers setting up a Google Account on their Android mobile phones and tablets, and to consumers who later accessed their Google Account settings through their Android mobile phones and tablets.

The ACCC stated that its "case regarding the collection of location data focuses on two Google Account settings: one labelled 'Location History'; and another labelled 'Web & App Activity'." The agency alleged "that from January 2017 until late 2018, it was misleading for Google to not properly disclose to consumers that both settings had to be switched off if consumers didn't want Google to collect, keep and use their location data.' The ACCC claimed that "when consumers set up a Google Account on their Android phone or tablet, consumers would have incorrectly believed, based on Google's conduct, that 'Location History' was the only Google Account setting that affected whether Google collected, kept or used data about their location." The agency further added that "if consumers later accessed their Google Account settings on their Android device,

Google did not inform them that by leaving 'Web & App Activity' switched on, Google would continue to collect location data."

The ACCC stated its allegations "that from around mid-2018 until late 2018, Google represented to consumers that the only way they could prevent Google from collecting, keeping and using their location data was to stop using certain Google services, including Google Search and Google Maps." The ACCC noted that "this could be achieved by switching off both 'Location History' and 'Web & App Activity'."

In terms of possible liability, since much of Google's alleged conduct occurred before a rewrite of the Australia Competition Law that will allow for higher possible fines, including up to 10% of annual turnover and/or A$10 million per violation, any possible fine could be relatively small (on the order of A$1.2 million per violation). This is not Google's first privacy violation fine this year. In January, France's Commission nationale de l'informatique et des libertés (CNIL) aka (the French Data Protection Authority) levied a €50 million fine under the General Data Protection Regulation (GDPR) "for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization." In September, the Federal Trade Commission (FTC) and New York Attorney General Leticia James announced a $170 million settlement with Google and its subsidiary YouTube regarding alleged violations of the "Children's Online Privacy Protection Act of 1998" (COPPA) and Section 5 of the FTC Act. To date, this is the largest settlement to resolve alleged COPPA violations.

Earlier this year, the ACCC released its final report from its "Digital Platforms Inquiry" that "proposes specific recommendations aimed at addressing some of the actual and potential negative impacts of digital platforms in the media and advertising markets, and also more broadly on consumers." Not surprisingly, the report focuses entirely on Facebook and Google but not Amazon, which the ACCC remarked was still relatively small in Australia.

Moreover, the ACCC explained

> Many digital platforms increasingly collect a large amount and variety of user data. The data collected often extends far beyond the data users actively provide when using the digital platform's services. Digital platforms may passively collect data from users, including from online browsing behaviour across the internet, IP addresses, device specifications and location and movement data. Once collected, digital platforms often have broad discretions regarding how user data is used and also disclosed to third parties.

The ACCC articulated its "view that consumers' ability to make informed choices is affected by:

- The information asymmetry between digital platforms and consumers. The ACCC found that consumers are generally not aware of the extent of data that is collected nor how it is collected, used and shared by digital platforms. This is influenced by the length, complexity and ambiguity of online terms of service and privacy policies. Digital platforms also tend to understate to consumers the extent of their data collection practices while overstating the level of consumer control over their personal user data.

Facebook Settles With The UK's DPA

The United Kingdom's Information Commissioner's Office (ICO) settled its investigation into Facebook's use of and involvement with Cambridge Analytica and Global Science Research during

the 2016 Brexit vote and that year's U.S. election. Had the ICO's action been brought under the General Data Protection Regulation (GDPR) the ultimate fine would have likely been much larger, but the conduct in question occurred before the GDPR's effective date. Instead, the ICO was working under the Data Protection Act 1998 which provided less authority for fines. This settlement follows the July settlement with the Federal Trade Commission (FTC) regarding much of the same conduct for $5 billion.

In 2018 the ICO issued a monetary penalty notice (MPN) against Facebook for £500,000 that the company appealed and the ICO lost in the first court. After the agency filed an appeal, Facebook and the ICO have agreed to settle, and Facebook has agreed to pay the £500,000 fine but has made no admission of liability in relation to the MPN.

In the MPN, the ICO explained that:

> (1) The Facebook Companies unfairly processed personal data, in breach of the first data protection principle set out in Schedule 1 to the DPA; and
> (2) The Facebook Companies failed to take appropriate technical and organizational measures against unauthorised or unlawful processing of personal data in breach of the seventh data protection principle set out in Schedule 1 to the DPA.

The ICO continued by noting that "[t]he Commissioner's view is that, in all the circumstances, each of these failures constituted a serious contravention by each of the Facebook companies…[and] further considers that the conditions for issuing a monetary penalty are satisfied and that it is appropriate to issue such a penalty in this case." The ICO added the "Commissioner considers that the amount of £500,000 is not excessive: indeed, but for the statutory limitation on the amount of monetary penalty, it would have been reasonable and proportionate to impose a higher penalty."

In its November 2018 report to Parliament titled "Investigation into the use of data analytics in political campaigns", the ICO explained

> One key strand of our investigation involved allegations that an app, ultimately referred to as 'thisisyourdigitallife', was developed by Dr Aleksandr Kogan and his company Global Science Research (GSR) in order to harvest the data of up to 87 million global Facebook users, including one million in the UK. Some of this data was then used by Cambridge Analytica, to target voters during the 2016 US Presidential campaign process.

In its July 2018 report titled "Democracy disrupted? Personal information and political influence," the ICO explained

- The online targeted advertising model used by Facebook is very complex, and we believe a high level of transparency in relation to political advertising is vital. This is a classic big-data scenario: understanding what data is going into the system; how users' actions on Facebook are determining what interest groups they are placed in; and then the rules that are fed into any dynamic algorithms that enable organisations to target individuals with specific adverts and messaging.
- Our investigation found significant fair-processing concerns both in terms of the information available to users about the sources of the data that are being used to determine what adverts they see and the nature of the profiling taking place. There were further concerns about the availability and transparency of the controls offered to users over what ads and messages they receive. The controls were difficult to find and were not intuitive to the user

if they wanted to control the political advertising they received. Whilst users were informed that their data would be used for commercial advertising, it was not clear that political advertising would take place on the platform.

- The ICO also found that despite a significant amount of privacy information and controls being made available, overall they did not effectively inform the users about the likely uses of their personal information. In particular, more explicit information should have been made available at the first layer of the privacy policy. The user tools available to block or remove ads were also complex and not clearly available to users from the core pages they would be accessing. The controls were also limited in relation to political advertising.

EC Finds That Voluntary Code To Combat Political Disinformation

The European Commission (EC) has released the "first annual self-assessment reports by Facebook, Google, Microsoft, Mozilla, Twitter and 7 European trade associations under the Code of Practice on Disinformation" according to a press release. This Code was drafted by technology companies and the advertising industry in response to a series of EC reports and statements on the disinformation campaigns waged by Russia and other nations.

In their statement on the self-assessment reports, Commissioner for Justice, Consumers and Gender Equality Věra Jourová, Commissioner for the Security Union Julian King, and Commissioner for the Digital Economy and Society Mariya Gabriel stated that "progress varies a lot between signatories and the reports provide little insight on the actual impact of the self-regulatory measures taken over the past year as well as mechanisms for independent scrutiny." The Commissioners claimed that "[m]ain findings from the self-assessment reports

- Compared to October 2018, the signatories to the Code of Practice indicate improved transparency. There is a closer dialogue with platforms as regards their policies against disinformation.
- While progress has been reported on the commitments monitored by the Commission from January to May ahead of the 2019 European Parliament elections, less is reported on the implementation of the commitments to empower consumers and the research community. The provision of data and search tools is still episodic and arbitrary and does not respond to the needs of researchers for independent scrutiny.
- The scope of actions undertaken by each platform to implement their commitments vary significantly. Similarly, differences in implementation of platform policy, cooperation with stakeholders and sensitivity to electoral contexts persist across Member States.
- The reports provide information on policies implementing the Code, including EU-specific metrics. The consistency and level of detail varies. The metrics provided are mainly output indicators, e.g. number of accounts taken down."

In the EC's analysis of the reports, the Commission contended that

> Reported actions taken by the platform signatories vary in terms of speed and scope across the five pillars of the Code as well as across the signatories. In general, actions to empower consumers and the research community lag behind the commitments, which were subject to the Commission's targeted monitoring phase towards the European Parliament elections in May 2019. The latter concern the disruption of advertising and monetization incentives for purveyors of disinformation, the transparency of political and issue-based advertising, and the integrity of services against inauthentic accounts and behaviours.

In April 2018, the EC published a communication in which it claimed "while the protection of the electoral process lies primarily within the competence of Member States, the cross-border dimension of online disinformation makes a European approach necessary in order to ensure effective and coordinated action and to protect the EU, its citizens, its policies and its Institutions." The communication explained "the views of the Commission on the challenges associated with disinformation online…[and] outlines the key overarching principles and objectives which should guide actions to raise public awareness about disinformation and tackle the phenomenon effectively, as well as the specific measures which the Commission intends to take in this regard.

Facebook and WhatsApp Sue Israeli Security Firm

WhatsApp and Facebook filed suit against the Israeli security firm, NSO Group, alleging that in April 2019, it sent "malware to approximately 1,400 mobile phones and devices…designed to infect the Target Devices for the purpose of conducting surveillance of specific WhatsApp users." This step was taken, Facebook and WhatsApp claim, in order to circumvent WhatApp's end-to-end encryption. The social media companies are suing "for injunctive relief and damages pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502, and for breach of contract and trespass to chattels."

Facebook and WhatsApp asserted

> Defendants took a number of steps, using WhatsApp servers and the WhatsApp Service without authorization, to send discrete malware components ("malicious code") to Target Devices. First, Defendants set up various computer infrastructure, including WhatsApp accounts and remote servers, used to infect the Target Devices and conceal Defendants' identity and involvement. Second, Defendants used and caused to be used WhatsApp accounts to initiate calls through Plaintiffs' servers that were designed to secretly inject malicious code onto Target Devices. Third, Defendants caused the malicious code to execute on some of the Target Devices, creating a connection between those Target Devices and computers controlled by Defendants (the "remote servers"). Fourth, on information and belief, Defendants caused Target Devices to download and install additional malware—believed to be Pegasus or another remote access trojan developed by Defendants—from the remote servers for the purpose of accessing data and communications on Target Devices.

Facebook and WhatsApp further alleged that those people targeted by NSO Group

> had WhatsApp numbers with country codes from several countries, including the Kingdom of Bahrain, the United Arab Emirates, and Mexico. According to public reporting, Defendants' clients include, but are not limited to, government agencies in the Kingdom of Bahrain, the United Arab Emirates, and Mexico as well as private entities.

In a *Washington Post* op-ed, WhatsApp head Will Cathcart claimed

> As we gathered the information that we lay out in our complaint, we learned that the attackers used servers and Internet-hosting services that were previously associated with NSO. In addition, as our complaint notes, we have tied certain WhatsApp accounts used during the attacks back to NSO. While their attack was highly sophisticated, their attempts to cover their tracks were not entirely successful.

Cathcart claimed the attack "targeted at least 100 human-rights defenders, journalists and other members of civil society across the world." He stated that "[t]his should serve as a wake-up call for technology companies, governments and all Internet users…[and] [t]ools that enable surveillance into our private lives are being abused, and the proliferation of this technology into the hands of irresponsible companies and governments puts us all at risk."

Last month, the American Civil Liberties Union (ACLU) published a report detailing "targeted digital attacks against two prominent Moroccan Human Rights Defenders (HRDs) using NSO Group's Pegasus spyware. " The ACLU said "these targeted attacks have been ongoing since at least 2017…[and] were carried out through SMS messages carrying malicious links that, if clicked, would attempt to exploit the mobile device of the victim and install NSO Group's Pegasus spyware."

Wyden/Eshoo Letter to Barr on Encryption

Senator Ron Wyden (D-OR) and Representative Anna Eshoo (D-CA) sent a letter to Attorney General William Barr in response to an October letter sent by Barr and other American, British, and Australian officials pressing Facebook to abandon plans to implement end-to-end encryption on all its messaging services.

Wyden and Eshoo stated

> Child sexual abuse imagery (CSAI) is a plague that companies, government and civil society groups must work together to purge from our society. However, we have serious concerns about the Department of Justice's (DOJ) misguided, hypocritical efforts to pressure technology companies like Facebook into subverting the encryption that protects their messaging apps to enable government access. This proposal will not meaningfully address the problem of CSAI, because illegal content will simply move to the dark web and to foreign commercial providers that are beyond the reach of U.S. law enforcement, while exposing millions of law-abiding Americans to new cybersecurity threats from stalkers, hackers and other criminals.

Wyden and Eshoo noted "Congress passed the PROTECT Act of 2008 and the Child Protection Act of 2012, both of which require DOJ to take steps to coordinate a cross-sectoral approach to reducing CSAI. They stated that "[u]nfortunately, DOJ has failed to comply with parts of these laws, including a requirement that it submit to Congress a National Strategy for Child Exploitation Prevention and Interdiction every two years." Wyden and Eshoo stated that "[f]urther, experts have highlighted several immediate steps law enforcement agencies can take to increase their ability to use digital evidence, beyond stopping encryption."

As mentioned, early last month, the U.S., U.K., and Australia sent Facebook an "open letter" regarding the company's March announcement that it would be "implementing end-to-end encryption for all private communications," asking that the company "not proceed with its plan...without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens." The three nations asked "that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens." The officials claimed

> Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes. This puts our citizens and societies at risk by severely eroding a company's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse, terrorism, and foreign adversaries' attempts to undermine democratic values and institutions, preventing the prosecution of offenders and safeguarding of victims. It also impedes law enforcement's ability to investigate these and other serious crimes.

FCC Order and Report on Huawei and ZTE

Federal Communications Commission (FCC) Chair Ajit Pai released a draft Report and Order that "would prohibit companies from using money from the FCC's $8.5 billion Universal Service Fund (USF) to purchase equipment or services from any company that poses a national security threat" and "would initially designate two Chinese companies—Huawei and ZTE Corporation—as companies that pose a national security risk and would establish a process for designating additional covered companies in the future" according to a fact sheet. This rule is prospective, so it affects future uses of USF funds to buy or maintain telecommunications equipment. Moreover, the final Report and Order follows a 2018 notice of proposed rulemaking (NPRM) titled "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs" the agency undertook after Congress directed federal agencies to stop buying Huawei and ZTE products and services pending the promulgation of regulations.

Moreover, Pai released with the draft Report and Order, "a draft Further Notice of Proposed Rulemaking (NPRM) and draft Information Collection Order would propose to remove and replace equipment produced by covered companies from USF-funded communications networks." This NPRM would entail

- An assessment to find out how much Huawei and ZTE equipment is in these networks and the costs to remove and replace it; and
- Financial assistance to carriers to help them transition to more trusted suppliers.

The FCC is expected to take up these items, among others, at a November 19 meeting.

The FCC explained that

> In 2018, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA). Section 889(b)(1) of the 2019 NDAA prohibits the head of an executive agency from obligating or expending loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system. Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services" as (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the

> Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country, where "covered foreign country" is defined as the People's Republic of China.

Regarding Huawei and ZTE, the FCC contended that "[b]oth companies' ties to the Chinese government and military apparatus—together with Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their systems—pose a threat to the security of communications networks and the communications supply chain and necessitate taking this step."

The FCC stated

> Since its inception, the USF has operated as one of the primary mechanisms for achieving this mission. The Commission provides monetary support through four separate but complementary USF programs: (1) the high cost program, which provides support to eligible carriers that provide service to high-cost areas, thereby making voice and broadband service affordable for residents living in such regions; (2) the Lifeline program, which assists eligible low income customers by helping to pay for monthly telephone and broadband charges; (3) the rural health care program, which helps subsidize rates for telecommunications and broadband services to health care facilities in rural areas; and (4) the E-Rate program, which provides support for broadband, internal connections, and other services to eligible schools and libraries.

The FCC stated

- Based on our review of the extensive record in this proceeding, we adopt a rule that no universal service support may be used to purchase or obtain any equipment or services produced or provided by a covered company posing a national security threat to the integrity of communications networks or the communications supply chain. Accordingly, USF recipients may not use USF funds to maintain, improve, modify, operate, manage, or otherwise support such equipment or services in any way, including upgrades to existing equipment and services.
- In addition to adopting this rule, we initially designate Huawei Technologies Company and ZTE Corporation as covered companies for the purposes of this prohibition. Both companies' ties to the Chinese government and military apparatus—together with Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their systems—pose a threat to the security of communications networks and the communications supply chain and necessitate taking this step. Our actions today are informed by the evidence cited herein, including the actions of other agencies and branches of the government and similar assessments from other countries.

The FCC claimed that "[t]oday's Report and Order marks an important step towards securing our nation's telecommunications networks and supply chains from national security threats…[and] [a]t the same time, we recognize that further steps are needed to secure our communications networks." Consequently, the FCC proposed "to require as a condition on the receipt of any USF support that eligible telecommunications carriers (ETC) not use or agree to not use within a designated period of time, communications equipment or services from covered companies." The agency stated that "[i]n addition to conditioning future USF support, we propose to require ETCs receiving USF support to remove and replace covered equipment and services from their network operations." The FCC

stated that "[t]o mitigate the impact on affected entities, and in particular small, rural entities, we propose to establish a reimbursement program to offset reasonable transition costs." The FCC proposed "to make the requirement to remove covered equipment and services by ETCs contingent on the availability of a funded reimbursement program…[and] expect[s] these proposals would facilitate the ETC transition of their equipment and services to safer and more secure alternatives and seek comment on these proposals."

At least one of the FCC Commissioners was critical of how Pai has handled this rulemaking. In testimony discussing 5G and national security before the Senate Homeland and Governmental Affairs Committee, FCC Commissioner Jessica Rosenworcel claimed

> At the Federal Communications Commission we have a rulemaking to ensure that our USF, which provides billions annually to support broadband deployment in rural communities, going forward will not be used to purchase insecure network equipment. That rulemaking has inexplicably stalled for more than a year and a half. But now, perhaps because you announced this hearing, we have publicized that we will vote on this in three short weeks.

Further Reading

- "I Accidentally Uncovered a Nationwide Scam on Airbnb" – *Vice*. A writer discovered through experience about a scam many on the short-term rental site, Airbnb, have experienced: a last-minute cancellation leading to a much inferior property and an interminable process for lodging complaints and obtaining a refund. Airbnb seems lax about enforcing its own policies against deceptive properties, and the incentive structure is weighted against renters leaving candid reviews.
- "An Unidentified Government Spied On Dissidents In India Using A WhatsApp Exploit" – *BuzzFeed News*. Israel's NSO Group's spyware may have been used by India's ruling Bharatiya Janata Party (BJP) to surveil judges, activists, academics, journalists, and politicians by exploiting a weakness in WhatsApp, a messaging application used by more than 400 million Indians. This is, of course, not the first time the NSO Group has been linked to spyware, and in this case, the spyware, Pegasus, was inserted on phones through a call made using WhatApp to the victim's phone they did not even need to answer. India's Home Ministry has denied any connection and calls the reports "attempts to malign the government of India," and the NSO Group seemed to claim that any such uses of its technology are contrary to their intended uses.
- "Police want faster data from the US, but Australia's encryption laws could scuttle the deal" – *ABC (Australia)*. As the U.S. and Australia negotiate a CLOUD Act agreement that would provide each country with a legal process to obtain information on citizens from technology companies as part of a law enforcement investigation, concerns and reservations are being raised in both countries about the powers of the Australian government under the "Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" that allows it to direct technology companies to provide assistance in decrypting user information without any judicial review.
- "Missouri Official Admits to Tracking Women's Periods" – *The Cut*. Health & Senior Services Director Dr. Randall Williams admitted during a hearing that his office maintained a spreadsheet with women's menstrual cycles drawn from medical information the state had access to. He further admitted the database was used to track "failed abortions" as a means of investigating abortion and reproductive services clinics.

- "Russia Tests New Disinformation Tactics in Africa to Expand Influence" – *The New York Times*. Facebook and Stanford's Internet Observatory revealed vast, new evolved Russian disinformation efforts being deployed in Africa with the goal of bringing successful tactics to the U.S. for next year's election. For now, these tactics seem to boost Russian interests in the region and call into question American and French actions. The volume of both disinformation creation and distribution have increased several times compared to the 2016 U.S. election. These efforts have been tied to Yevgeny Prigozhin, the Russian oligarch who runs the Internet Research Agency and is a close ally of Vladimir Putin.
- "Gaggle Knows Everything About Teens And Kids In School" – *BuzzFeed News* and "School apps track students from classroom to bathroom, and parents are struggling to keep up" – *The Washington Post*. Two articles on the technology that many public schools are employing to track kids in the physical and digital worlds, begging many questions about the long term effect on children, their privacy, their rights, and their lives.
- "A Chinese hacking group breached a telecom to monitor targets' texts, phone metadata" – *cyberscoop*. APT41 compromised a telecommunications company in a strategic competitor of China's and surveilled a range of people. The Chinese hackers infected devices using SMS.
- "Banks are using their Washington clout to stomp on the tech industry" – *Politico*. As if the tech industry isn't having enough trouble in Washington, the lobbies representing the banks and other financial services entities have worked to block cryptocurrencies and tech's entry into any sector of banking and finance and found willing allies on Capitol Hill.