Michael Kans' Technology Policy Update
12 September 2019
By Michael Kans, Esq.

Spotlight: A Privacy Bill A Week

Last week, we took a look at a House bill, the "Information Transparency & Personal Data Control Act" (H.R. 2013) which is sponsored by Suzan DelBene (D-WA) and cosponsored by 22 other House Democrats. This week, we will examine one of the Senate bills sponsored by Senators Marsha Blackburn (R-TN), Tammy Duckworth (D-IL), and Martha McSally (R-AZ): the "Balancing the Rights Of Web Surfers Equally and Responsibly Act of 2019" (BROWSER Act) (S. 1116). S. 1116 would set up an enhanced notice and consent regime for consumers policed by the Federal Trade Commission (FTC) but only for certain classes of private sector entities collecting, sharing, selling, and using consumer information, mainly broadband providers and so-called "edge Providers," that is entities like Google and Facebook that provide services online. This bill is much closer to the current FTC means for regulating privacy and data security even though the scope of the agency's jurisdiction to police privacy practices for some types of consumer information would be expanded.

As noted, this bill would cover only "broadband internet access service[s]" and "edge service[s]," which as these terms are defined in the bill would mostly be technology and communications companies. Therefore, this bill would sweep much more narrowly than many of the other privacy bills introduced thus far. Accordingly, S. 1116 defines "broadband internet access service" as "a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service." The bill also provides a definition of "edge service:" "a service provided over the internet—

> for which the provider requires the user to subscribe or establish an account in order to use the service;
> that the user purchases from the provider of the service without a subscription or account;
> by which a program searches for and identifies items in a database that correspond to keywords or characters specified by the user, used especially for finding particular sites on the world wide web; or
> by which the user divulges sensitive user information; and
> includes a service described in subparagraph (A) that is provided through a software program, including a mobile application.

Clearly, big technology companies like Facebook, Google, Instagram, Amazon, etc. would be classified as "edge providers." Moreover, the definition of broadband internet access service would clearly include all of the internet service providers like Comcast or AT&T but would also seem to include cell phone service providers like Verizon and T-Mobile.

All covered service providers must "provide a user of the service with clear and conspicuous notice of the privacy policies of the provider with respect to the service." Additionally, covered service providers must also give users "clear and conspicuous advance notice of any material change to the privacy policies of the provider with respect to the service."

Whether consumers need to opt-in or opt-out on data use will turn on whether the information is "sensitive" or not. Under S. 1116, "sensitive user information" includes any of the following:

- Financial information.
- Health information.
- Information pertaining to children under the age of 13.
- Social Security number.
- Precise geolocation information.
- Content of communications.
- Web browsing history, history of usage of a software program (including a mobile application), and the functional equivalents of either.

Among the information that would be deemed non-sensitive under the bill are meta-data (aka call detail records) from usage of a phone such as the addressee of a communication and the time, one's order history from a site like Amazon, matters relating to employment, and other categories of information not enumerated above. Additionally, the bill deems "precise geolocation information" as sensitive information, suggesting "geolocation information" that is less than precise might be non-sensitive. So, perhaps a trip to a mall would not be considered "precise" but the stores a customer visits might be?

Covered service providers would need to "obtain opt-in approval from a user to use, disclose, or permit access to the sensitive user information of the user." However, what constitutes the "approval" necessary to satisfy this requirement is not spelled out in the bill. Conversely, the provider of covered services must only offer consumers the option to opt out of the use, disclosure, and accessing of their non-sensitive personal information. Again "approval" is a key word as covered service providers need only obtain a consumer's approval in order to opt-out.

As is usually the case, there are some exceptions to this seemingly general rule against using, collecting, sharing, or selling sensitive user information. Notably, in the following situations, covered service providers need not obtain opt-in approval from consumers:

> (1) In providing the covered service from which the information is derived, or in providing services necessary to, or used in, the provision of the service.
> (2) To initiate, render, bill for, and collect for the covered service.
> (3) To protect the rights or property of the provider, or to protect users of the covered service and other service providers from fraudulent, abusive, or unlawful use of the service.
> (4) To provide location information or non-sensitive user information—
>
> > (A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the request of the user for emergency services;
> > (B) to inform the legal guardian of the user, or members of the immediate family of the user, of the location of the user in an emergency situation that involves the risk of death or serious physical harm; or
> > (C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.
>
> (5) As otherwise required or authorized by law.

Covered service providers would not be able to require consumers to waive their privacy rights in exchange for use of a service. The bill stipulates that "[a] provider of a covered service may not—

(1) condition, or effectively condition, provision of the service on agreement by a user to waive privacy rights guaranteed by law or regulation, including this Act; or
(2) terminate the service or otherwise refuse to provide the service as a direct or indirect consequence of the refusal of a user to waive any privacy rights described in paragraph (1)."

The FTC would enforce this new privacy scheme under its existing Section 5 powers to police unfair and deceptive practices and crucially not as if a violation of an existing FTC regulation against unfair and deceptive practices. If the FTC is seeking to punish a violation of such a regulation, it may seek civil fines in the first instance. And, this is in contrast to the FTC's general powers to punish unfair and deceptive practices with respect to data security and privacy violations, which is limited to monetary remedies in the form of equitable relief such as disgorgement and restitution. The BROWSER Act would be at odds with most other privacy bills that contain language such as "[a] violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices."

Again unlike other bills, the BROWSER Act does not provide the FTC with the authority to promulgate regulations under the Administrative Procedures Act (APA) process, and to the extent the agency would be able to write regulations to implement the bill, it would be under the much more lengthy and involved Moss-Magnuson procedures that have effectively halted the FTC's regulatory activity (*see* "It's Time to Remove the "Mossified" Procedures for FTC Rulemaking" for a summary of these procedures.) Therefore, the FTC would essentially extend to privacy regulation its current practice of penalizing companies for not maintaining "reasonable" data security standards on a case-by-case basis and not providing any bright lines to assure companies of the practices.

The FTC's jurisdiction would be expanded, however, to police the privacy practices under the bill for broadband providers that would otherwise be subject to the jurisdiction and enforcement powers of the Federal Communications Commission (FCC.)

The bill would preempt state privacy laws. To wit, "[n]o State or political subdivision of a State shall, with respect to a provider of a covered service subject to this Act, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the privacy of user information." Of course, preemption of state laws is a non-starter for many Democrats but a sine non qua for many Republicans, leaving this as an area of ongoing dispute.

Regarding another issue that has split Democrats and Republicans in the past regarding data security legislation, the BROWSER Act would not provide a role for state attorneys general to enforce the new regulatory regime. However, Republicans may be willing to give on this issue provided consumers have no private right of action, and the BROWSER Act would not allow consumers to sue those providing covered services for violating the bill.

Fall Preview For Technology Legislation

With Congress having returned from the August recess, bright-eyed and bushy-tailed, a host of bills are awaiting these eager lawmakers. However, I will focus only on those bills that have been marked up and reported out of committee or have been passed by one chamber as these bills may be the most likely to be enacted. Of course, there are other issue areas Congress may address with

legislation this fall, but as yet, legislation has neither been introduced nor marked up (e.g. privacy, data security, and the PATRIOT Act reauthorization.)

First, and possibly foremost, since this reauthorization has been enacted annually since the Kennedy Administration, is the FY 2020 National Defense Authorization Act (NDAA) (H.R. 2500/S. 1790). As cybersecurity has grown in prominence nationally and at the Pentagon, provisions dealing with this topic area have proliferated. Consequently, both bills are stuffed with statutory language ranging from supply chain to acquisition to offensive and defensive cyber operations, and other facets of cybersecurity. Likewise, the committee reports are also full of directives , mainly to the Pentagon, regarding actions, programs, briefings, and reports Congress would like the Department of Defense to undertake. Both NDAAS have passed their respective chambers and the Armed Services Committees have been working on reconciling the bills. Incidentally, the Senate attached its FY 2018, 2019, and 2020 Intelligence Authorization to S. 1790, which is also replete with cyber-related provisions for the Intelligence Community (i.e. the "Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020" (S. 1589)). On July 17, the House passed the "Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act (IAA) for Fiscal Years 2018, 2019, and 2020" (H.R. 3494) by a 397-31 vote. Therefore, it is possible that the NDAA also carries the intelligence reauthorization to enactment.

Speaking of annually enacted vehicles to effect technology policy, all twelve of the FY 2020 appropriations acts have yet to be enacted. A. number of the bills contain crucial language on cybersecurity and technology funding with a handful of bills being most important with respect to funding: the Homeland Security, Department of Defense, Financial Services and General Government, and the Commerce-Justice-Science appropriations acts. Despite having struck a deal on top-lines, it is not clear that Congress will enact of its appropriations bills before the current year ends on September 30. Therefore, we may be looking a continuing resolution into the fall, ideally followed by an omnibus or series of bills packaged together to fund FY 2020 programs. For example, the "FY 2020 Homeland Security Appropriations Act" would provide the Cybersecurity and Infrastructure Security Agency (CISA) $2.016 billion for FY 2020, a boost of $334 million above its FY 2019 funding level and $408 million above the Administration's budget request."

Election security will likely be an area around which there will be intense messaging but less legislative action. House Democrats made election security reform a policy priority in large part because of the Russian interference and hacking in the 2016 election. The House has sent substantially the same legislation in two bills (i.e. the "For The People Act of 2019" (H.R. 1), a package of election reforms, and the "Securing America's Federal Elections (SAFE) Act of 2019" (H.R. 2722)) to the Senate where Senate Majority Leader Mitch McConnell (R-KY) has refused to consider them or Senate bills. Broadly speaking these bills would authorize funding and establish federal standards for states and localities in improving and upgrading their election systems from hacks and attacks. Incidentally, the $600 million in election grants these bills call for was provided in the "Financial Services and General Government Appropriations Act, 2020" (H.R. 3351) the House passed in June.

As noted, at the end of July, after the Senate Intelligence Committee released the first of the five volume report on the 2016 presidential election, Senators Richard Blumenthal (D-CT), Mark Warner (D-VA), Amy Klobuchar (D-MN), and others sought unanimous consent to proceed to a number of election security related bills but were blocked by Senate Republicans. The bills Senate Democrats tried to bring up for immediate consideration included:

- The "Duty To Report Act" (S. 1247)

- The "FIRE Act" (S. 2242)
- The "Senate Cybersecurity Protection Act" (S. 890)
- The "Securing America's Federal Elections Act" (SAFE Act) (H.R. 2722)

The Senate did, however, pass the "Defending the Integrity of Voting Systems Act" (S. 1321) by unanimous consent on July 17. S. 1321 would "make it a federal crime to hack any voting systems used in a federal election" according to the Senate Judiciary Committee's website. In June the Senate also passed the "Defending Elections against Trolls from Enemy Regimes (DETER) Act" (S. 1328) that "will make "improper interference in U.S. elections" a violation of U.S. immigration law, and violators would be barred from obtaining a visa to enter the United States. The House has yet to act on these bills. However, despite action on S. 1321 and 1328, Senate Democrats seem intent on continuing to try and force consideration of election security legislation. It is unclear whether McConnell will relent.

Likewise, the House has also began legislation to punish those found guilty of interfering with U.S. elections. In July the House Foreign Affairs Committee met and marked up a number of bills, including: the "Safeguard our Elections and Combat Unlawful Interference in Our Democracy Act" (SECURE Our Democracy Act) (H.R. 3501) "would impose sanctions on anyone found to interfere illegally in an American election from overseas…[and] is designed to punish Russian interference in the 2016 election and also deter future election interference" according to the Committee's press release.

Congress also has pending a number of bills focused on the federal government's cybersecurity posture and capabilities. In January, the House passed the "Federal CIO Authorization Act of 2019" (H.R. 247) that would codify the positions of Chief Information Officer (CIO) and Chief Information Security Officer (CISO), make the positions presidential appointments, require the CIO to report directly to the Office of Management and Budget (OMB) Director, require each agency to submit reports on all IT expenditures to the CIO, and task the CIO with submitting a plan to Congress "for consolidating information technology across the Federal Government...and increasing the use of shared services, including any recommendations for legislative changes that may be necessary to effect the proposal." H.R. 247 is identical to a bill, the "Federal CIO Authorization Act of 2018" (H.R. 6901), the House overwhelmingly passed in December, but the Senate never took up the bill.

On July 17, the House Homeland Security Committee held a markup and reported out four such cybersecurity bills:

- The "Securing the Homeland Security Supply Chain Act of 2019" (H.R. 3320) would "authorize the Secretary of Homeland Security to implement certain requirements for information relating to supply chain risk" with authority similar to those granted to the Department of Defense in the FY 2019 National Defense Authorization Act to exclude contractors with unacceptable supply chain risks.
- The "DHS Acquisition Reform Act of 2019" (H.R. 3413) would "provide for certain acquisition authorities for the Under Secretary of Management of the Department of Homeland Security."
- The Pipeline Security Act (H.R. 3699) would "codify the Transportation Security Administration's responsibility relating to securing pipelines against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of pipelines."
- The "Cybersecurity Vulnerability Remediation Act" (H.R. 3710) would permit but not require the Cybersecurity and Infrastructure Security Agency (CISA) to "identify, develop, and

disseminate actionable protocols to mitigate cybersecurity vulnerabilities, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor."

In June, the House took up and passed the "DHS Cyber Incident Response Teams Act of 2019" (H.R. 1158), as amended, by voice vote. H.R. 1158 would require the Cybersecurity and Infrastructure Security Agency's (CISA) National Cybersecurity and Communications Integration Center (NCCIC) to "maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance "to asset owners and operators in restoring services following a cyber incident" among other circumstances. NCCIC must "continually assess and evaluate the cyber incident response teams and their operations using robust metrics" and may "include cybersecurity specialists from the private sector on cyber hunt and incident response teams." A related bill has been marked up and reported out of the Senate Homeland Security and Governmental Affairs Committee, the "DHS Cyber Hunt and Incident Response Teams Act of 2019" (S. 315), that would charge NCCIC and CISA with substantially the same missions. The Senate Homeland Security Committee marked up and reported out two other such bills:

- The "National Cybersecurity Preparedness Consortium Act of 2019" (S. 333) would allow the Department of Homeland Security to "work with a consortium to support efforts to address cybersecurity risks and incidents." Consortiums are defined to be "a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security."
- The "Federal Rotational Cyber Workforce Program Act of 2019" (S. 406), which would establish a program under which cybersecurity employees would rotate at federal agencies.

In July, the Senate Homeland Security Committee marked up and reported out the "State and Local Government Cybersecurity Act of 2019" (S. 1846) that would provide the Department of Homeland Security (DHS) the authority "[t]o make grants to and enter into cooperative agreements or contracts with States, local governments, and other non-Federal entities" and direct the National Cybersecurity and Communications Integration Center (NCCIC) to work with "with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center" on addressing a variety of cybersecurity-related responsibilities.

Congress also has proposed measures targeted at small businesses. On July 15, the House took and passed a pair of cybersecurity bills from the suspension calendar:

- The "SBA Cyber Awareness Act" (H.R. 2331) would "require the Small Business Administrator (SBA) to issue annual reports assessing its IT and cybersecurity infrastructure and notify Congress and affected parties of cyber incidents when they occur."
- The "Small Business Development Center Cyber Training Act of 2019" (H.R. 1649) "help Small Business Development Centers (SBDCs) become better trained to assist small businesses with their cyber security and cyber strategy needs…[and] would establish a cyber counseling certification program in lead SBDCs to better assist small businesses with planning and implementing cybersecurity measures to defend against cyber attacks."

Congress has also initiated legislation to better regulate the energy sector's cybersecurity. On July 17, the House Energy and Commerce Committee marked up a quartet of energy sector cybersecurity bills:

- The "Enhancing Grid Security through Public-Private Partnerships Act" (H.R. 359) "directs the Secretary of Energy, in consultation with States, other federal agencies, and industry

stakeholders, to create and implement a program to enhance the physical and cyber security of electric utilities.

- The "Cyber Sense Act of 2019" (H.R. 360) would establish "voluntary program [that] would identify cyber-secure products that could be used in the bulk- power system."
- The "Energy Emergency Leadership Act" (H.R. 362) would "create a new DOE Assistant Secretary position with jurisdiction over all energy emergency and security functions related to energy supply, infrastructure, and cybersecurity."
- The "Pipeline and LNG Facility Cybersecurity Preparedness Act" (H.R. 370) "would establish a program at DOE, in coordination with other Federal agencies, States, and the energy sector, to create policies and procedures to improve the physical and cyber security and resiliency of natural gas transmission and distribution pipelines, hazardous liquid pipelines, and liquefied natural gas (LNG) facilities."

There are two bills regarding the Internet of Things that have been reported out of committee. On July 10, the Senate Commerce, Science, and Transportation Committee held a markup and reported out the "Developing Innovation and Growing the Internet of Things (DIGIT) Act" (S. 1611) sponsored by Senators Deb Fischer (R-NE), Cory Gardner (R-CO), Brian Schatz (D-HI), and Cory Booker (D-NJ). In her press release, Fischer explained the bill would "would convene a working group of federal entities and experts from the private and academic sectors tasked with providing recommendations to Congress on how to facilitate the growth of connected Internet of Things (IoT) technologies." She added that "[t]he group's recommendations would focus on how to plan for, and encourage, the development and deployment of the IoT in the U.S…[and] directs the Federal Communications Commission (FCC) to complete a report assessing spectrum needs required to support the Internet of Things." S. 1611 is substantially similar to legislation (S. 88) the Senate passed unanimously in the last Congress the House never took up. It is not clear whether the same resistance exists in the House, but unlike the last Congress a companion DIGIT Act has not yet been introduced in the House.

Earlier this year, two versions of the same IoT bill were marked up and reported out of committee. The Senate Homeland Security and Governmental Affairs Committee marked up and reported out the "Internet of Things Cybersecurity Improvement Act of 2019" (S. 734) a week after the House Oversight and Reform Committee acted on the "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668) after adopting an amendment in the nature of a substitute that narrowed the scope of the bill. In general, these bills seek to leverage the federal government's ability to set standards through acquisition processes to ideally drive the development of more secure IoT across the U.S. The stakeholders are responding to the security risks presented by weak or nonexistent security for IoT as seen in a number of major malware attacks. The legislation would require the NIST, the OMB, and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to work together to institute standards for IoT owned or controlled by most federal agencies. These standards would need to focus on secure development, identity management, patching, and configuration management and would be made part of Federal Acquisition Regulations (FAR), making them part of the federal government's approach to buying and utilizing IoT. Thereafter, federal agencies and contractors would need to use and buy IoT that meets the new security standards.

Finally, House Democrats have made rolling back the Federal Communications Commission's (FCC) repeal of the Obama Administration's Open Internet Order (aka net neutrality) a priority. On April 3, the House Energy and Commerce Committee marked up and reported out the "Save the Internet Act of 2019" (H.R. 1644) that would undo the Federal Communications Commission's (FCC) repeal

of the Obama Administration's 2015 net neutrality order and reclassify internet service providers (ISPs) under Title II of the Federal Communications Act as common carriers. The bill was subsequently passed by the House by a 232-190 vote, but the Senate has not yet taken up the bill and likely will not.

State AGs Launch A Facebook Probe

New York Attorney General Leticia James announced a "bipartisan" investigation of "social media giant Facebook for antitrust issues." James is acting in concert with the attorneys general of Colorado, Florida, Iowa, Nebraska, North Carolina, Ohio, Tennessee, and the District of Columbia, and their investigation will "focus[] on Facebook's dominance in the industry and the potential anticompetitive conduct stemming from that dominance." James declared that "[w]e will use every investigative tool at our disposal to determine whether Facebook's actions may have endangered consumer data, reduced the quality of consumers' choices, or increased the price of advertising."

This investigation follows the U.S. Department of Justice's (DOJ) July announced review of "whether and how market-leading online platforms have achieved market power and are engaging in practices that have reduced competition, stifled innovation, or otherwise harmed consumers." The DOJ's "review will consider the widespread concerns that consumers, businesses, and entrepreneurs have expressed about search, social media, and some retail services online." The DOJ's "Antitrust Division is conferring with and seeking information from the public, including industry participants who have direct insight into competition in online platforms, as well as others." Given Facebook's dominance as an online platform, it is all but certain the DOJ will be examining their practices for anti-competitive behavior. Moreover, the other federal anti-trust regulator has apparently also launched an inquiry in Facebook. In its Quarter 2 earnings press release, the social media giant revealed "[i]n June 2019, we were informed by the FTC that it had opened an antitrust investigation of our company."

Facebook faces another federal action. In April, 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.

The New York Attorney General's office has announced two other such investigations into Facebook over the last two years, neither of which has yet resulted in criminal or civil action. In April, James announced an investigation "into Facebook's unauthorized collection of 1.5 million Facebook users' email contact databases." James asserted that "Facebook has repeatedly demonstrated a lack of respect for consumers' information while at the same time profiting from mining that data." Similarly, former New York Attorney General Eric Schneiderman issued a 2018 press release on an investigation into Facebook and Cambridge Analytica regarding the use of Facebook users' information and data during the 2016 presidential campaign.

NTIA Issues First Annual Report on the Status of Spectrum Repurposing; Several Other 5G Reports Propose Policy Directions

The Department of Commerce, acting through the National Telecommunications and Information Administration (NTIA), released its initial annual report "on the status of existing efforts and planned near- to mid-term spectrum repurposing initiatives" as required by an October 2018 Presidential Memorandum "on Developing a Sustainable Spectrum Strategy for America's Future." This report and other initiatives form the Trump Administration's efforts to move the U.S. to 5G networks in a way that maintains American national security through continued technological dominance. This is, of course, a response to China's avowed ambition to displace the U.S. as the world's engine of technological development, specifically through seeking to dominate certain sectors of the technology field including 5G, semiconductors, artificial intelligence, and others.

Accordingly, in the report, NTIA explained

> This report is part of a broader effort to maintain the U.S. position as a global leader in pioneering and sustaining technological and economic leadership in developing and deploying spectrum-dependent products and services, from 5G wireless systems to innovative satellite and space applications. A significant component of this effort is the construction and execution of the National Spectrum Strategy called for by the *Presidential Memorandum*. The U.S. Government will continue to support this leadership in ground-breaking wireless technologies, including those that greatly improve the spectrum efficiency and effectiveness of federal operations. This is being accomplished through ongoing efforts to assess the Nation's spectrum needs and to identify additional bands with federal and non-federal allocations to serve those needs. This will entail examining and implementing effective protective measures for incumbent services and managing the transitions as spectrum uses shift and new spectrum-sharing tools and techniques are developed and implemented. These ongoing efforts constitute a process that resembles a "pipeline" for continuous identification and assessment of bands, followed by repurposing or implementing other spectrum access mechanisms wherever needed and feasible.

In terms of other, pending actions regarding spectrum, the EO also requires

> Within 270 days of the date of this memorandum, the Secretary [of Commerce], working through the NTIA, and in consultation with he Office of Management and Budget (OMB), the Office of Science and Technology Policy (OSTP), and the Federal Communications Commission (FCC), and other Federal entities, as appropriate, shall submit to the President, through the Director of the National Economic Council and the Assistant to the President for National Security Affairs, a long-term National Spectrum Strategy that includes legislative, regulatory, or other policy recommendations

The NTIA is the latest in a line of reports as policymakers are trying to address the myriad challenges posed by the move to 5G.

In July, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released an assessment that "Fifth Generation Mobile Network (5G) will present opportunities and challenges, and its implementation will introduce vulnerabilities related to supply chains, deployment, network security, and the loss of competition and trusted options.

- Use of 5G components manufactured by untrusted companies could expose U.S. entities to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by poor manufacturing processes and maintenance procedures.

5G hardware, software, and services provided by untrusted entities could increase the risk of compromise to the confidentiality, integrity, and availability of network assets. Even if U.S. networks are secure, U.S. data that travels overseas through untrusted telecommunication networks is potentially at risk of interception, manipulation, disruption, and destruction.

- 5G will use more components than previous generations of wireless networks, and the proliferation of 5G infrastructure may provide malicious actors more attack vectors. The effectiveness of 5G's security enhancements will in part depend on proper implementation and configuration.
- Despite security enhancement over previous generations, it is unknown what new vulnerabilities may be discovered in 5G networks. Further, 5G builds upon previous generations of wireless networks and will initially be integrated into 4G Long-Term Evolution (LTE) networks that contain some legacy vulnerabilities.
- Untrusted companies may be less likely to participate in interoperability efforts. Custom 5G technologies that do not meet interoperability standards may be difficult to update, repair, and replace. This potentially increases the lifecycle cost of the product and delays 5G deployment if the equipment requires replacement. The lack of interoperability may also have negative impacts on the competitive market as companies could be driven out if the available competitive market decreases.

CISA explained that "[t]he United States Government can manage these vulnerabilities and increase the security of communications networks as 5G is adopted by:

- Encouraging continued development of trusted 5G technologies, services, and products.
- Encouraging continued trusted development of future generations of communications technologies.
- Promoting international standards and processes that are open, transparent, consensus–driven, and that do not place trusted companies at a disadvantage.
- Limiting the adoption of 5G equipment with known or suspected vulnerabilities.
- Continued engagement with the private sector on risk identification and mitigation efforts.
- Ensuring robust security capabilities for 5G applications and services.

Also, in July, the Defense Science Board, a venerated advisory body, released the executive summary of the report submitted by its Quick Task Force (TF) on Defense Applications of 5G Network Technology that "was established to define a path for potential DOD 5G adoption that mitigates supply chain risk, establishes spectrum co-existence procedures and revamps existing communication infrastructure." The TF "concludes that there can be significant benefits from using 5G technology in the DOD but inherent supply chain, cyber, Radio Frequency (RF)/Electronic Warfare (EW) and virtual/physical vulnerabilities create significant mission risk." The TF claimed that "[a]ny deployment of 5G in DOD infrastructure must be measured against mission criticality and acceptable risk."

The TF made the following findings:

Finding 1: 5G Bandwidth (BW) and services, low power implementations and low latency capabilities may enhance DoD current mission capabilities and have potential to create new mission capabilities.

- Multiple strategies for adopting 5G must be considered
- Insufficient 5G resources and testbed(s) capable of evaluating current and proposed standards, capabilities and technologies exist

Finding 2: While 5G largely evolves from 4G, much has changed – significant shifts in IP, authorities in standards development and supply chain have occurred.

- 5G capability is inexorably intertwined with leading edge microelectronics
- Much activity was observed with little coordination and a lack of strategic direction
- China is known to influence/coordinate positions before major standards decisions and seeks to control future standards

Finding 3: Inherent supply chain, cyber, RF/EW and virtual/physical vulnerabilities create significant mission risk.

- The lack of a U.S. integrator and Radio Access Network (RAN) vendor industrial base creates challenges
- Continuous testing and experimentation can help mitigate risk while creating new opportunities
- Findings and recommendations from the DSB's earlier and current cyber studies apply

Finding 4: Network function virtualization, new radio, security enhancements present mission opportunities.

- New spectrum and new radio capabilities create opportunities for increased spectrum sharing, high BW transmission with Low-Probability-of-Intercept (LPI)/Low-Probability-of-Detection (LPD)/Low-Probability-of-Jamming (LPJ) characteristics
- 5G security enhancements provide an added layer of protection over 4G
- 5G commercial satellite options have the potential to create unprecedented opportunities for global communications

Finding 5: New and emerging technology presents an opportunity to regain leadership for future 3rd Generation Partnership Project (3GPP) standards releases.

- Ultra-densification of cellular networks with heavy reliance on small, micro- and pico cells will create new mission opportunities
- Artificial Intelligence (AI) and machine learning in the protocol stack will enhance performance
- Design and fabrication of components at commercial timescale can be applied to antenna arrays

Finding 6: 5G Deployment must be measured against mission criticality and acceptable risk.

The TF made the following recommendations:

Recommendation 1: Adopt 5G for military use in lightly contested environments.
Recommendation 2: Develop a secure 5G system for contested environments and critical applications.
Recommendation 3: Create test beds for exploring innovative use cases.
Recommendation 4: Stand-up a telecommunications security program.
Recommendation 5: Develop a DoD 5G supply chain management strategy.
Recommendation 6: Create a program for "vulnerability analysis."
Recommendation 7: Develop and execute a 3 year 5G+ S&T roadmap.
Recommendation 8: Develop a 5G+ Standards Engagement Plan.
Recommendation 9: Establish a new bi-direction spectrum sharing paradigm.
Recommendation 10: Accelerate mmWave technology development and transition.

In April, an advisory body to the Pentagon drafted a report on the options facing the Department of Defense (DOD) as the U.S. and other nations are on the cusp of transitioning to the next generation of wireless networks that promise even faster speeds that will likely drive the development of new applications and devices. The Defense Innovation Board (Board) released "THE 5G ECOSYSTEM: RISKS & OPPORTUNITIES FOR DOD" to "insight into the commercial landscape as well as the DOD landscape to give a comprehensive view of the stakeholders and future of 5G." The Board explained that "[t]he shift from 4G to 5G will drastically impact the future of global communication networks and fundamentally change the environment in which DOD operates." The Board conceded that "[w]hile DOD will feel the impact of 5G, the rollout itself will be driven by the U.S. commercial sector."

The Board explained

> The term "5G" refers to the oncoming fifth generation of wireless networks and technology that will produce a step-change improvement in data speed, volume, and latency (delay in data transfer) over fourth generation (4G and 4G LTE) networks. 5G will enable a host of new technologies that will change the standard of public and private sector operations, from autonomous vehicles to smart cities, virtual reality, and battle networks. Historical shifts between wireless generations suggest that the first-mover country stands to gain billions in revenue accompanied by substantial job creation and leadership in technology innovation. First movers also set standards and practices that were then adopted by subsequent entrants. Conversely, countries that fell behind in previous wireless generation shifts were obligated to adopt the standards, technologies, and architectures of the leading country and missed out on a generation of wireless capabilities and market potential.

The development of 5G will require the bonding together of 100 MHz channels to deliver faster speeds in new spectrums. The Board explained that the U.S., Japan, and South Korea are looking at using the electromagnetic spectrum frequencies between 24 and 300 GHz (aka mmWave) for 5G while other nations, like China, are looking at using the 3 and 4 GHZ range (aka sub-6) for 5G networks. Moreover, in the U.S., the DOD uses the latter spectrum, meaning that any transition could be tricky for 5G using that band of spectrum. The Board noted that "U.S. carriers are primarily focused on mmWave deployment for 5G because most of the 3 and 4 GHz spectrum being used by the rest of the world for 5G are exclusive Federal bands in the United States, extensively used by DOD in particular."

FTC and NY AG Levy Largest COPPA Fine Ever on Google and YouTube

Last week, 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. However, the FTC split 3-2 along party lines to approve the settlement.

As explained in the complaint, COPPA "applies to any operator of a commercial website or online service directed to children under 13 years of age that collects, uses, and/or discloses personal information from children, or on whose behalf such information is collected or maintained. Personal information is "collected or maintained on behalf of an operator when . . . [t]he operator benefits by allowing another person to collect personal information directly from users of such Web site or

online service." COPPA also "requires a covered operator to give notice to parents and obtain their verifiable consent before collecting children's personal information online."

The FTC and Attorney General Leticia James claimed that

> commercial entities operating child-directed "channels" on Defendants' YouTube platform are "operators" under the COPPA Rule, as they permit Defendants to collect personal information, such as persistent identifiers for use in behavioral advertising, on behalf of those commercial entities. In numerous instances, Defendants have actual knowledge they are collecting personal information directly from users of these child-directed channels. Through this actual knowledge, Defendants are deemed to be operators of a website or online service directed to children. At no time have Defendants attempted to provide parents with the COPPA-specified notice of their information practices or obtain verifiable parental consent.

In the settlement, the FTC and Attorney General Leticia James explained that Google, YouTube, and others "are permanently restrained and enjoined from:

- Failing to develop, implement, and maintain a system for Channel Owners to designate whether their Content on the YouTube Service is directed to Children. Such system shall include a Clear and Conspicuous notice that Content made available on the YouTube Service that is directed to Children may be subject to the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312…and that Channel Owners are obligated to designate such Content as directed to Children;
- Failing to provide annual training regarding complying with the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312…for each Person responsible for managing Defendants' relationships with Channel Owners on the YouTube Service.
- Failing to make reasonable efforts, taking into account available technology, to ensure that a Parent of a Child receives direct notice of Defendants' practices with regard to the Collection, use, or Disclosure of Personal Information from Children, including notice of any material change in the Collection, use, or Disclosure practices to which the Parent has previously consented, unless the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312…provides an exception to providing such notice;
- Failing to post a prominent and clearly labeled link to an online notice of its information practices with regard to Children on the home or landing page or screen of its website or online service, and at each area of the website or online service where Personal Information is Collected from Children, unless the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312…provides an exception to providing such notice;
- Failing to Obtain Verifiable Parental Consent before any Collection, use, or Disclosure of Personal Information from Children, including consent to any material change in the Collection, use, or Disclosure practices to which the Parent has previously consented, unless the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312…provides an exception to Obtaining Verifiable Parental Consent; and
- Violating the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312

The settlement further stipulates

> that Defendants, Defendants' officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this

> Order, are ordered to refrain, within ninety (90) days of the Compliance Date, from Disclosing, using, or benefitting from Personal Information previously Collected from users of Content that is designated as directed to Children by a Channel Owner under the system required under Section I.A. above, as long as such designation occurs within sixty (60) days of the Compliance Date. Provided, however, that such Personal Information may be Disclosed to the extent requested by a government agency or required by law, regulation, or court order.

Of the $170 million, $136 million goes to the FTC and $36 million goes to the New York Attorney General. To put the fine in context, Google's most recent 10-Q showed $10.636 billion in net income for the second quarter of 2019.

The FTC Commissioners issued four different statements making their cases as to why the settlement was justified or not. This split echoes the split in the settlement with Facebook with the Democratic Commissioners arguing for a larger fine while the Republican majority touted the historic size of the settlement and the provisions put in place to govern the company's conduct going forward.

FTC Chair Joe Simons and Commissioner Christine Wilson issued a joint statement highlighting what they saw as "the most significant aspects of the settlement:

- First, it requires Defendants to pay $136 million to the FTC and $34 million to New York. The $170 million total monetary judgment is almost 30 times higher than the largest civil penalty previously imposed under COPPA. This significant judgment will get the attention of platforms, content providers, and the public.
- Second, the settlement includes strong conduct relief that goes beyond the technical requirements of COPPA. Indeed, as Commissioner Slaughter notes, this relief will change YouTube's business model going forward. Under COPPA, third parties that host and serve ads on child-directed content – but do not themselves create the content – are not responsible for making inquiries about whether the content is child-directed. This settlement now makes Defendants responsible for creating a system through which content creators must self-designate if they are child-directed. This obligation exceeds what any third party in the marketplace currently is required to do. It represents the first and only mandated requirement on a platform or third party to seek actual knowledge of whether content is child-directed.
- Third, the complaint alleges two first impression applications of COPPA.
    - First, the complaint alleges that individual channels on a general audience platform are "websites or online services" under COPPA. This framing puts content creators and channel owners on notice that we consider them to be standalone "operators" under COPPA, subject to strict liability for COPPA violations.
    - Second, the complaint alleges that YouTube has liability under COPPA as a third party. When the Commission amended the COPPA Rule in 2013, we stated that platforms are not generally responsible for child-directed content that appears on them, unless the platform possesses actual knowledge that it is collecting personal information from users of a child directed site or service. As detailed in the complaint, YouTube did possess actual knowledge as evidenced by its own marketing efforts, information received from channels, and its review of channel content to curate for the YouTube Kids App.

As noted, the FTC split along party lines with the two Democratic Commissioners voting against the settlement and issuing dissenting statements. Commissioner Rohit Chopra offered a summary of his full dissent:

- For the third time since 2011, the FTC is sanctioning Google for privacy violations. This latest violation is extremely serious. The company baited children using nursery rhymes, cartoons, and other kid-directed content on curated YouTube channels to feed its massively profitable behavioral advertising business.
- Illegally harvesting children's data was extremely lucrative. It generated short-term profits and advanced its long-term dominance in the children's video market. Google knew that content on YouTube channels was directed to young children, but did not disable illegal data collection.
- The FTC frequently points to its insufficient authority to protect the privacy of Americans, but when it comes to children, the Commission already has strong tools provided by the COPPA. Despite this specific authority, the Commission repeats many of the same mistakes from the flawed Facebook settlement: no individual accountability, insufficient remedies to address the company's financial incentives, and a fine that still allows the company to profit from its lawbreaking. The terms of the settlement were not even significant enough to make Google issue a warning to its investors.
- The approach in this matter is inconsistent with other children's privacy enforcement actions against small companies, where individuals are closely scrutinized and settlement terms are crippling. This outcome reinforces my concerns that the Commission brings down the hammer on small firms, while allowing large firms to get off easier.

Moreover, Chopra noted that had the FTC used a methodology similar to its 2012 "action against Google, [where] the FTC obtained a penalty of more than five times the company's unjust gains," the settlement would have likely been billions of dollars.

Chopra added

> If Congress enacts privacy legislation, it should not cut and paste COPPA's approach to penalties. It should move away from vague factors for civil penalties and shift toward ones that are easier for agencies and courts to administer. There are many alternative approaches, such as requiring a minimum penalty per violation, adjusted upward if the violation is intentional or reckless. In addition, Congress should give all enforcers of any privacy law a robust set of enforcement tools, including penalties. In COPPA, state attorneys general can only seek forfeiture of ill-gotten gains and refunds to victims, but not financial penalties beyond that. In this matter, the New York Attorney General was unable to pursue civil penalties, since the FTC has exclusive authority to do so. This should change.

Letters To Amazon Regarding The Safety Of Items Sold In Its Marketplace

In response to the Wall Street Journal's (WSJ) article, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products", which found that Amazon's quality and safety control was allowing items to be sold by third-party vendors that failed to meet federal safety standards, two Democratic letters were sent to Amazon seeking answers. Moreover, to date, there has been no public indication that the primary federal regulator of many consumer goods, the Consumer Product Safety Commission (CPSC), that the agency is investigating some of the non-compliant goods the WSJ highlighted in its expose. However, the article and the letters might spur

Congressional action in the form of hearings or even an update of the CPSC's enabling statute, which Congress last revised over ten years ago.

Senators Bob Menendez (D-NJ), Richard Blumenthal (D-CT), and Ed Markey (D-MA) wrote to Amazon CEO and Chairman Jeff Bezos "with grave concerns regarding Amazon's failure to remove from its platform illegal, deadly, and deceptive products, and to provide required visible warnings on products sold on your platform. " They urged Amazon "to take swift action to provide accurate warnings that protect consumers against these dangerous and deadly products and to stop their wrongful sale."

Menendez, Blumenthal, and Markey stated

> Even when Amazon has banned products, its monitoring appears to be inadequate. In certain instances, although Amazon has claimed it has banned many of these unsafe products, they still remain widely and easily accessible on the platform. In one particularly egregious example, in 2012, Amazon reportedly restricted the sale of powerful magnetic balls and cubes that the Consumer Product Safety Commission deemed a "substantial product hazard." When more than one magnet is swallowed, they can snap together rupturing a child's digestive organs. However, the WSJ report found for sale on your platform 80 different listings of these magnets that should not be available.

The Senators stated that "[a]s you know, it is illegal to sell recalled items under the Consumer Product Safety Improvement Act of 2008, and violators can face civil penalties up to $15 million." Menendez, Blumenthal, and Markey added that "[w]e acknowledge that it is individual retailers' responsibility to ensure that the products they sell are legal…[b]ut many of the faulty products tested by the WSJ were shipped from Amazon warehouses and labeled as "Amazon's Choice" — a seeming endorsement of the products."

Menendez, Blumenthal, and Markey requested "answers to the following questions:

1. Why have your current safety efforts failed to prevent the sale of mislabeled, recalled, and other unsafe products?
2. How will you now ensure that you will not sell recalled products or other products deemed unsafe by the National Highway Transportation Safety Administration, the Food and Drug Administration, the Consumer Protection Safety Commission, or any other federal agency?
3. How will you identify all products that should include required choke hazard and other warning labels, for example, balloons?
4. How will you ensure that all such identified products will include accurate required warning labels?
5. How will you ensure that products on your platform meet minimum safety requirements and do not violate existing law, including, for example, lead limits in children's products?
6. What assurances will you give that the technology and analytics you develop to address these issues will continue to protect consumers as new products and new safety standards are developed?

Representative Grace Meng (D-NY) also wrote to Bezos "[a]s the founder and Co-Chair of the Congressional Kids Safety Caucus," "to address the disturbing reports that items found on the Amazon Marketplace are non-compliant with federal regulations." She urged Bezos to "create more transparency in your Marketplace and create plans to remove recalled or unsafe products." Meng asked for "answers to the following questions:

- Will you cease to sell products on the Amazon Marketplace that have been recalled by their manufacturers for safety concerns?
- What is your timeline and process to ensure these products are entirely and promptly removed from your Marketplace?
- How will you create more transparency to help customers understand which products on your Marketplace are sold by third-party companies?
- How will you increase the monitoring of products being listed falsely as FDA compliant?"

Federal Energy Regulators Propose Naming Non-Compliant Electric Utilities

The Federal Energy Regulatory Commission (FERC) issued a staff white paper developed with the North American Electric Reliability Corporation (NERC) on "Notices Of Penalty Pertaining To Violations Of Critical Infrastructure Protection Reliability Standards." Despite this seemingly innocuous title lies what may be a controversial regulatory approach: naming utilities that violate cybersecurity standards. FERC explained that the proposed approach would name the violators, the specific Critical Infrastructure Protection (CIP) reliability standards breached, and the penalties being assessed. The CIP reliability standards "contain requirements that provide for the cybersecurity of the Bulk-Power System."

As explained in FERC's press release, "[t]he joint staff white paper proposes to provide transparency and public access to information on violations of mandatory reliability standards governing cybersecurity of the bulk electric system while protecting sensitive information that could jeopardize security."

In the white paper, FERC and NERC staff explained

> The significant increase in FOIA requests for non-public information in CIP NOPs has raised security and transparency concerns within industry and the general public, which has prompted Commission and NERC staffs to re-evaluate the format of CIP Notices of Penalties (NOPs) filed with the Commission. The current filing format, containing detailed violation information, when coupled with the potential release of unidentified registered entity (URE) identities, may not be achieving an appropriate balance of security and transparency.

The FERC and NERC staff "propose[d] a revised format that is intended to improve this balance." They stated that "[s]pecifically, under the proposal, NERC CIP NOP submissions would consist of a proposed public cover letter that discloses the name of the violator, the Reliability Standard(s) violated (but not the Requirement), and the penalty amount. " The staffs stated that "NERC would submit the remainder of the CIP NOP filing containing details on the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems as a non-public attachment, along with a request for the designation of such information as Critical Energy/Electric Infrastructure Information (CEII)." The FERC and NERC staff stated that "[t]his proposal would allow for transparency related to the identity of the entity and violation while protecting the more sensitive security information that could jeopardize the security of the Bulk-Power System."

Further Reading

- "Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran" – *Yahoo News*. "For years, an enduring mystery has surrounded the Stuxnet virus attack that

targeted Iran's nuclear program: How did the U.S. and Israel get their malware onto computer systems at the highly secured uranium-enrichment plant?" Turns out it was a Dutch-recruited insider that allowed Stuxnet to be turned loose by providing know-how and access.

- "NASA Astronaut Accused Of Hacking Bank Account From Space" – *Forbes*. In what may be the first cyber crime from space, an astronaut admitted to accessing her estranged spouse's bank account, but it is not clear if she committed a crime.
- "NATO WILL DEFEND ITSELF: The alliance will guard its cyber domain—and invoke collective defence if required" – *Prospect*. NATO Secretary General Jens Stoltenberg explained in an op-ed that "a serious cyberattack could trigger Article 5 of our founding treaty…where an attack against one ally is treated as an attack against all." He added that "[w]e have designated cyberspace a domain in which NATO will operate and defend itself as effectively as it does in the air, on land, and at sea." Stoltenberg stated that "[t]his means we will deter and defend against any aggression towards allies, whether it takes place in the physical world or the virtual one."
- "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks" – *ProPublica*. "The FBI and security researchers say paying ransoms contributes to the profitability and spread of cybercrime and in some cases may ultimately be funding terrorist regimes. But for insurers, it makes financial sense, industry insiders said. It holds down claim costs by avoiding expenses such as covering lost revenue from snarled services and ongoing fees for consultants aiding in data recovery. And, by rewarding hackers, it encourages more ransomware attacks, which in turn frighten more businesses and government agencies into buying policies."
- "Business Email Compromise overtakes ransomware and data breaches in cyber-insurance claims" – *ZDNet*. However, ransomware may soon be eclipsed by a different type of hack: Business email compromise (BEC). According to AIG, BEC "has overtaken ransomware and data breaches as the main reason companies filed a cyber-insurance claim in the EMEA (Europe, the Middle East, and Asia) region last year."
- "The World's First Ambassador to the Tech Industry" – *The New York Times*. In a sign of how Silicon Valley is perceived throughout the world and its actual importance, Denmark appointed the first Tech Ambassador."
- "As bounty hunters buy our digital footprints, FCC drags its feet" – *Boston Globe*. Representative Lori Trahan (D-MA) and Federal Communications Commission (FCC) Commissioner Jessica Rosenworcel press the FCC to act on the selling of phone geolocation. "Our phones know our location at any given moment. This geolocation data is especially sensitive. It's a record of where we've been, and by extension, who we are. This information needs to be treated with care. If it winds up in the wrong hands, it could provide criminals and stalkers with the ability to locate any one of us with pinpoint accuracy. It could be sold to domestic abusers or anyone else who wishes to do us harm. Its collection and distribution or sale without our permission is a violation of our most basic privacy norms.
- "California adopted the country's first major consumer privacy law. Now, Silicon Valley is trying to rewrite it." – *The Washington Post*. Not surprisingly, many companies and sectors of the economy have been lobbying hard in Sacramento to amend, and critics say weaken, the "California Consumer Privacy Act" (CCPA) (AB 375). We will soon see if they succeed in this session.
- "Facebook Lays Out Challenges of Letting Users Take Their Data to Other Platforms" – *The Wall Street Journal*. Facebook's new white paper "Charting a Way Forward on Privacy and Data Portability" tries to navigate the seemingly contradictory goals of protecting user privacy and promoting and allowing data portability.

- "Connected Cars Race to Market, Raising Cybersecurity Fears" – *KQED*. Like any other internet-connected device, automobiles can be hacked, a situation likely to get worse as more and more connected cars come into use.
- "NSA: Just say no to hacking back" – *FCW*. The National Security Agency's chief counsel warns private sector entities against going on the offensive against hackers and thieves. Rather they should leave the response to the professionals at the FBI or DHS.
- "How Kentucky Gambled for Hundreds of Millions of Dollars From a Broadband Program It Didn't Qualify for" – *ProPublica*. A cautionary tale ProPublica has been investigating in detail. Kentucky tried to secure federal grant funds for KentuckyWired to match private funds, and it basically all went very, very wrong. Now, Kentucky does not have broadband, and it is on the hook for over $500 million.
- "New York City sues T-Mobile over 'rampant' customer sales abuses" – *Reuters*. A New York City consumer protection agency sues T-Mobile over the alleged illegal and unethical practices of its subsidiary Metro.
- "Amazon's Next-Day Delivery Has Brought Chaos And Carnage To America's Streets — But The World's Biggest Retailer Has A System To Escape The Blame" – *BuzzFeed News*. The human cost of doorstep delivery from Amazon.
- "Why is the Russian meddling in 2016 such a big secret? I'm not allowed to say." – *The Washington Post*. In an op-ed, Representative Stephanie Murphy (D-FL) discusses what she can about Russian efforts to target Florida during the 2016 presidential election and why U.S. law enforcement agencies will not get into specifics publicly.
- "DMVs Are Selling Your Data to Private Investigators" – *Motherboard*. Apparently, many motor vehicle administrations are selling taxpayers' personal data for profit.