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

Spotlight: A Privacy Bill A Week

Last week, we dove into the "Balancing the Rights Of Web Surfers Equally and Responsibly Act of 2019" (BROWSER Act) (S. 1116). This week, we'll look at another bipartisan Senate bill but one sponsored by a contestant for the Democratic nomination: Senator Amy Klobuchar (D-MN). She introduced the "Social Media Privacy Protection and Consumer Rights Act of 2019" (S. 189) with Senator John Kennedy (R-LA) in January 2019. Broadly speaking, under this bill the major tech companies would need to give consumers an opportunity to opt in or opt out of the company's data usage practices after offering enhanced notice of the practices for which the personal data may used.

The bill would cover only "online platforms" which are defined as "any public-facing website, web application, or digital application (including a mobile application); and includes a social network, an ad network, a mobile operating system, a search engine, an email service, or an internet access service." However, the bill would encompass a subset of "online platforms" (i.e. those that "collect[] personal data during the online behavior of a user of the online platform." Consequently, it appears that a company like Amazon with a huge online presence would not be considered an online platform. The same would seem to be true of any other retailer with an online presence that falls short of being one of the specified types of online platform.

Moreover, it is not clear under the bill that all of the practices of online platforms that impinge privacy would be covered by the bill. The use of the phrase "during the online behavior of a user of the online platform" raises the possibility that some online platforms may claim that some instances of data collection of online behavior may not be covered by the bill, or it may be suggested that certain behaviors are off-line. For example, in a May article, the *Washington Post's* technology columnist found that at 3:00 am his iPhone is "beaming out lots of information about me to companies I've never heard of" "[e]ven though the screen is off and I'm snoring." I suppose one could make the case that even though he was not online, the apps he downloaded were. However, it is more logical to say he was not online, so should the Klobuchar-Kennedy bill be enacted as written, this would seem to be data collection outside the bounds of the privacy regime. Also, how would cookies be treated? Conceivably once a consumer has logged off of Facebook, should the platform's cookies continue to pipe information back to the company? Or is this the sort of behavior one could consent to?

S. 189 defines personal data more narrowly than some of the other bills. For example, most telephone metadata would fall outside the bounds of what is considered personal data except for geolocation data, so a consumer's privacy choice would be functionally meaningless for this type of data. In the same vein, location information other than that could be used to identify a street and a city would be fair game, so it appears online platforms could use and share less precise location information like just a town or a city.

Nonetheless, what is "personal data" is "individually identifiable information about an individual collected online, including—

(A) location information sufficient to identify the name of a street and a city or town, including a physical address;
(B) an email address;
(C) a telephone number;
(D) a government identifier, such as a Social Security number;
(E) geolocation information;
(F) the content of a message;
(G) protected health information, as defined in section 160.103 of title 45, Code of Federal Regulations, or any successor regulation; and
(H) nonpublic personal information, as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) (i.e. personally identifiable financial information…provided by a consumer to a financial institution…resulting from any transaction with the consumer or any service performed for the consumer…or…otherwise obtained by the financial institution."

When a person creates an account with an online platform, he must be given the option to choose between having his personal data collected and used by the online platform and third parties or declining to agree to such terms. However, nothings appears to be off limits in terms of collection and use of personal data once a consumer has consented to the terms the online platform offers. Once a consumer has agreed to the terms put forth by the online platform, then the platform is free to do what they will with user personal data so long as they are transparent about the uses and abide by their published privacy or security program.

The biggest possible loophole I see is if a user opts against an online platform from collecting and using her personal data, the platform "may deny certain services or completely deny access to the user" if the choice "creates inoperability in the online platform." How is inoperability to be defined? Could Facebook say that since so much of its business model is built on collecting and using personal data that when a user opts out, the platform then becomes inoperable? Since the FTC is not given authority to promulgate regulations under the Administrative Procedures Act, what constitutes bona fide "inoperability" will be determined on a case-by-case basis if the agency finds this term is being used in ways contrary to the intent of the law.

Nonetheless, a user may withdraw his consent at any time or in the event of a privacy violation. However, doing so would seem to implicate the same concern as an initial refusal to consent: the online platform may find such refusal creates inoperability problems, allowing them to deny services.

Of course an online platform must obtain consent or allow a consumer to opt-out when they create an account, but what of existing accounts with, say Facebook or Google. The bill would take effect six months after enactment, and it provides that "[a]n individual who becomes a user of a covered online platform before the effective date under subsection (a) shall be treated as if he or she had become a user of the online platform on that effective date." This would suggest that existing users would not be offered a choice as to whether they op-in or opt-out. However, such a user may withdraw consent after the effective date if they find the terms ion the newly revised notice to be objectionable.

There is language regarding the standards online platforms must meet in terms of the notice they provide consumers regarding the type of personal data collected and its uses. It must be
(I) easily accessible;
(II) of reasonable length; and

(III) clearly distinguishable from other matters; and
(ii) uses language that is clear, concise, and well organized, and follows other best practices appropriate to the subject and intended audience.

The bill requires online platforms to allow users to request and receive "a copy of the personal data of the user that the operator has processed, free of charge and in an electronic and easily accessible format, including a list of each person that received the personal data from the operator for business purposes, whether through sale or other means." However, there is no language on the timeframe by which the online platform should meet this request.

S. 189 would require covered online platforms to "establish and maintain a privacy or security program for the online platform" and to "publish a description of the privacy or security program." However, a plain reading of this requirement suggests that an online platform subject to S. 189 need only establish and maintain a "privacy ***or*** security program," meaning only one or the other. The rationale for giving online platforms a choice is not immediately clear. In any event, the online platform needs to also "publish a description of the privacy or security program that—

details how the operator will use the personal data of a user of the online platform, including requirements for how the operator will address privacy risks associated with the development of new products and services; and
includes details of the access that employees and contractors of the operator have to the personal data of a user of the online platform, and internal policies for the use of that personal data."

There appears to be an ill-defined incentive for online platforms to develop better technology to secure the privacy of consumers. If an online platform develops "privacy-enhancing technology," then it would not need to offer consumers a choice on data collection and usage, a copy of her data as processed and used, nor alert her in the event of a "privacy violation." However, the bill does not indicate what might qualify as "privacy-enhancing technology" except that this provision suggests that it applies to the "development" of this sort of technology. Presumably that would apply to yet-to-be developed technologies and seems to serve as an incentive for online platforms to put the time and resources into doing so. However, would encryption qualify as "privacy-enhancing technology"? This provision is vague so it is not clear.

Like virtually all the other privacy bills, the Federal Trade Commission (FTC) would treat all privacy violations as "a violation of a rule defining an unfair or deceptive act or practice," allowing the agency to seek civil fines of about $42,000 per violation in court as part of its immediate enforcement action. Common carriers and non-profits would be swept into the jurisdiction of the FTC for purposes of enforcing this act; however, only those "covered online platforms" that are also common carriers or non-profits would be subject to the bill. State attorneys general could enforce the regime in federal court so long as the FTC is not already doing so or does not seek to intervene. Also, the bill would not preempt state criminal and civil laws, so state attorneys general could simultaneously bring actions under state law at the same time the FTC is bringing an action in federal court.

Bills To Amend CCPA Go To Governor

The California legislature has finished its legislative work for the year absent extraordinary circumstances, and it passed six bills to amend the "California Consumer Privacy Act" (CCPA) (AB 375). However, a bill to exempt customer loyalty programs from the CCPA was not passed.

Governor Gavin Newsom has until October 13 to sign or veto the bills. However, regardless of what the Governor decides on these bills, these will almost certainly be the last amendments to the CCPA before it takes effect on January 1, 2020 because the legislature has adjourned for the year. Although it bears note that the date the new data privacy regime comes into full force will depend on when the California Attorney General's office issues regulations required by the bill.

As noted, the legislature passed these bills last week:

- A.B. 25 would exempt employers from the CCPA for only one year for activities related to collecting information from job applicants and employees.
- A.B. 1564 would revise a requirement in the CCPA for businesses to make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA.
- A.B. 1146 would "narrowly limit[] the CCPA's opt-out and deletion rights in order to facilitate prompt and effective recalls and warranty work" of automobiles.
- A.B. 1355 would address various drafting errors and make other clarifying changes in the California Consumer Privacy Act of 2018 (CCPA), notably to specify that "personal information" (as opposed to "publicly available") does not include consumer information that has been deidentified or aggregate consumer information. This bill would affect other changes, including widening an exception related to the Fair Credit Reporting Act and tightening the circumstances under which a consumer can sue a business in the event of a breach.
- A.B. 874 would expand the definition of "publicly available" information that is exempted from the definition of "personal information" (PI) in the CCPA to ensure that "publicly available" information includes any information that is lawfully made available from government records.
- A.B. 1202 would require data brokers to register with the Attorney General's office

It bears note that only AB 1355 and AB 1202 were subject to further changes after being sent to the Senate floor, and most notably, the small but significant change of greatest interest is the requirement that a consumer's personal information be both unecrypted and nonredacted in order for a consumer to sue if this information is improperly accessed. Currently the statute allows consumers to bring an action if their "nonencrypted or nonredacted" personal information "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." AB 1355 would require the personal information to be unencrypted and nonredacted before a suit can move forward. Consequently, businesses that fail in their duty to establish and operate reasonable data security practices and procedures and are breached would not be liable if the personal information in question is either encrypted or redacted.

As noted, the legislature declined to pass A.B. 846, a bill on how customer loyalty programs would be treated under the CCPA, even though it had been amended to narrow the scope of the exception. A.B. 846, as passed by the Assembly in May, would replace the "financial incentive programs" provisions in the nondiscrimination statute of the CCPA with an authorization for offerings that include, among other things, gift cards or certificates, discounts, payments to consumers, or other benefits associated with a loyalty or rewards program, as specified. However, the Senate Judiciary Committee narrowed this authorization, for opponents pointed out that the authorization served as a loophole under which personal information collected under these programs would functionally be exempted from the broader requirements of the CCPA. Consequently, companies operating loyalty

and rewards programs would not need to meet the consent and notice provisions in the CCPA. The amendment version of A.B. 846 specifies that the CCPA allows for loyalty or rewards programs and allows consumers using these programs to opt out of certain data collection and sale without facing adverse repercussions.

Now, the focus on CCPA will turn to the regulations the Attorney General's office (AG) has been working on to implement the CCPA. The first bill passed to amend the CCPA, last year's SB 1121, provided the AG "shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner." However, given that draft regulations have not yet been issued, it is looking likely that the effective date for the CCPA's enforcement provisions will be July 1, 2020. Also, Attorney General Xavier Becerra and his staff have stated in public, including committee hearings, that the AG's office lacks the staff and resources to bring many enforcement actions, so it is possible that, at first, the AG will only be able to focus his office's resources on a few major cases a year.

Final Rule Issued Banning Kaspersky

The Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) released a rule finalizing an interim regulation that "prohibits the use of products or services of Kaspersky Lab and its related entities by the Federal Government on or after October 1, 2018." This rule was effective upon being published, and the agencies explained they "are adopting as final, without change, an interim rule amending the Federal Acquisition Regulation (FAR) to implement a section of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018." This interim rule was promulgated in mid-2018.

Questions and concerns about Kaspersky's products began being raised in the course of the multiple investigations into Russian interference in the 2016 election. There were concerns that Kaspersky was either willing or unwittingly sharing information from U.S. systems with Russian Intelligence. In early to mid 2017, there were media reports based on classified documents shared with reporters posing further questions about how close Kaspersky was with the FSB. The heads of a number of intelligence agencies testified in an open hearing in May 2017 that they would not be comfortable with Kaspersky products on their systems.

In September of 2017, the Department of Homeland Security issued a binding operational directive (BOD) that obligated all federal agencies to initiative a process to remove most Kaspersky-branded products from their networks. However, this dictate did not apply to "national security systems," which is most of the DOD and the Intelligence Community. Moreover, the BOD did "not address Kaspersky code embedded in the products of other companies" and did "not address the following Kaspersky services: Kaspersky Threat Intelligence and Kaspersky Security Training."

However, in August 2019, a private security firm claimed "it has found software from Russian-based Kaspersky Labs present on multiple U.S. government networks and the networks of government contractors…[and] within a number of Fortune 500 companies, including 19 financial services companies and 17 healthcare businesses."

The "National Defense Authorization Act for Fiscal Year 2018" (P.L. 115-91) contained language from the Senate's NDAA "that would prohibit any department, agency, organization, or other element of the United States Government from using any product developed by Kaspersky Lab or any entity of which Kaspersky Lab has majority ownership" by October 1, 2018. The final language

in the enacted bill included those provisions but also required that the DOD and other agencies "review and report on the procedures for removing suspect products or services from the information technology networks of the Federal Government." To date, if this report has been completed, it has not been released.

Nonetheless, the DOD, GSA, and NASA promulgated an interim rule in June 2018 that took effect in July 2018. In the interim rule, the agencies explained that "[t]o implement section 1634, the clause at 52.204-23 prohibits contractors from providing any hardware, software, or services developed or provided by Kaspersky Lab or its related entities, or using any such hardware, software, or services in the development of data or deliverables first produced in the performance of the contract." The agencies added that "[t]he contractor must also report any such hardware, software, or services discovered during contract performance; this requirement flows down to subcontractors."

The DOD, GSA, and NASA also had to fill in gaps left by Congress in promulgating this ban, notably definitions for "covered entity" and "covered article," which were dealt with in the interim rule. Notably, the agencies drafted these definitions which were included in the final rule:

Covered article means any hardware, software, or service that—

(1) Is developed or provided by a covered entity;
(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or
(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

Covered entity means—

(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab;
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.

However, in the notice for the final rule, the agencies responded to comment from an industry stakeholder on “a specific list or definition around 'covered article' or 'covered entity.'" This stakeholder "also requested to share how and when an entity or article would be added to this list and incorporated into this clause.” The DOD, GSA, and NASA responded that "[d]ue to the continually evolving nature of technological product and service offerings, including third-party products that may either add or eliminate inclusion of elements such as Kaspersky Lab software, and the lack of suggestions for how this challenge might be managed, DOD, GSA, and NASA have concluded that providing a definitive list of hardware, software, or services subject to the definition of “covered article” is impractical, particularly in regulation." The agencies added that "[s]imilar challenges regarding the shifting nature of ownership, affiliate and subsidiary relationships also apply to the definition of “covered entity.” DOD, GSA, and NASA intend to confer with the Federal Acquisition Security Council staff as it considers issues related to the appropriate sharing of information to support management decisions associated with supply chain risk management."

Also, the agencies needed to determine whether the Kaspersky ban would apply to acquisitions of commercially available off-the-shelf (COTS) items and procurements at or below the simplified acquisition threshold (SAT). The Office of Management and Budget's (OMB) Office of Federal

Procurement Policy (OFPP) and the Federal Acquisitions Regulations Council determined that the ban would apply to both COTS and SAT acquisitions.

NIST's Releases First Draft of Privacy Framework

The National Institute of Standards and Technology (NIST) has released for comment the "Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management," (Preliminary Draft or Privacy Framework). Like the Cybersecurity Framework, the advice and guidance in the document are entirely voluntary, but also like that document, this NIST product could become the de facto standard for how private and public sector entities deal with privacy related to technology issues. Additionally, the Preliminary Draft is synced to the Cybersecurity Framework so that organizations can use the two documents in tandem. As NIST explains in the Preliminary Draft, "[w]hile managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise outside the scope of cybersecurity risks." NIST "is asking that all comments be submitted by October 24, 2019."

NIST developed the Preliminary Draft "using information collected through the Request for Information (RFI) that was published in the Federal Register on November 14, 2018, and a series of open public workshops and webinars...in collaboration with public and private stakeholders." NIST explained that "[i]t is intended for voluntary use to help organizations: Better identify, assess, manage, and communicate privacy risks when designing or deploying systems, products, and services; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in systems, products, and services."

The Preliminary Draft, as presented, is intended to provide an organizational tool for:

- Building customer trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;
- Helping to fulfill current compliance obligations, as well as future-proofing products and services in a changing technological and policy environment; and
- Facilitating communication about privacy practices with customers, assessors, and regulators.

NIST stated that "[i]t is designed to enable organizations to manage privacy risks through a prioritized, flexible, outcome-based, and cost-effective approach that is compatible with existing legal and regulatory regimes in order to be most useful to a broad range of organizations and enable widespread adoption." NIST noted that "[i]t is modeled after the structure of the Framework for Improving Critical Infrastructure Cybersecurity to facilitate the complementary use of both frameworks" and "is composed of three parts: the Core, Profiles, and Implementation Tiers."

In terms of its utility to help organizations manage privacy risks, NIST explained

> When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to optimize beneficial uses of data and the development of innovative systems, products, and services while minimizing adverse consequences for individuals. The Privacy Framework can help organizations answer the fundamental question, "How are we considering the impacts to individuals as we develop our systems, products, and services?" As a result, the Privacy Framework can serve as the foundation for a new privacy program or a mechanism for improving an existing program. In either case, it is designed to complement existing business and system development operations, to provide a means of

expressing privacy requirements to business partners and customers, and to support the identification of gaps in an organization's privacy practices.

NIST wants feedback on the following questions:

1. Does this preliminary draft:
    a. adequately define outcomes that:
        i. cover existing practices;
        ii. strengthen individuals' privacy protection;
        iii. enable effective organizational use;
        iv. support enterprise mission/business objectives; and
        v. facilitate compliance with applicable laws or regulations;
    b. appropriately integrate privacy risk into organizational risk;
    c. provide guidance about privacy risk management practices at the right level of specificity;
    d. adequately define the relationship between privacy and cybersecurity risk;
    e. provide the capability for those in different organizational roles such as senior executives and boards of directors, legal, compliance, security, and information technology or operations to understand privacy risks and mitigations at the appropriate level of detail;
    f. provide sufficient guidance and resources to aid organizations of all sizes to build and maintain a privacy risk management program while maintaining flexibility; and
    g. enable cost-effective implementation?
2. Will this preliminary draft, as presented:
    a. be inclusive of, and not disruptive to, effective privacy practices in use today, including widely used voluntary consensus standards that are not yet final;
    b. enable organizations to use the Privacy Framework in conjunction with the Framework for Improving Critical Infrastructure Cybersecurity to collaboratively address privacy and cybersecurity risks; and
    c. enable organizations to adapt to privacy risks arising from emerging technologies such as the Internet of Things and artificial intelligence?

Also, NIST released a document that "provides a mapping of the Subcategories in the Preliminary Draft Core to key relevant NIST guidance" such as the Special Publications the agency has issued on a range of related topics (e.g. SP 800-53 Rev. 5 (DRAFT), "Security and Privacy Controls for Information Systems and Organizations.")

Finally, should Congress fail to enact substantive, comprehensive privacy legislation, the Privacy Framework could be the federal government's de facto stance on privacy matters, especially since it appears that the National Telecommunications and Information Administration's (NTIA) attempt to develop an "approach to consumer data privacy" has stalled. As you may recall, "[i]n September 2018, the National Telecommunications and Information Administration (NTIA) issued a request for comments (RFC) "on a proposed approach to consumer data privacy designed to provide high levels of protection for individuals, while giving organizations legal clarity and the flexibility to innovate." However, in the meantime, NTIA head Dave Redl and other top NTIA officials stepped down, throwing into question the agency's focus on this initiative.

Schumer and Cotton Call For Agencies To Take Action on Chinese Companies

Senate Minority Leader Chuck Schumer (D-NY) and Senator Tom Cotton (R-AR) have sent a pair of letters to the Administration regarding two agencies' oversight of Chinese technology companies with ties to the Chinese military and government.

In the letter to Secretary of Defense Mark Esper, Schumer and Cotton were joined by Representatives Ruben Gallego (D-AZ) and Mike Gallagher (R-WI) in asking whether the Department of Defense (DOD) has been updating a list of "those persons operating directly or indirectly in the United States or any of its territories and possessions that are Communist Chinese military companies" as directed by Section 1237 of the FY 1999 NDAA. They noted that China's Communist Party has adopted a Military-Civilian Fusion strategy "to achieve its national objectives," including the acquisition of U.S. technology through any means such as espionage, forced technology transfers, and the purchase of or investment in U.S. technology forms. Schumer, Cotton, Gallego, and Gallagher urged the Trump Administration "reexamine all statutory authorities at its disposal to confront the CCP's strategy of Military-Civilian Fusion, including powers that have laid dormant for years."

Unstated in this letter, however, is that the first part of Section 1237 grants the President authority to "exercise International Emergency Economic Powers Act (IEEPA) authorities (other than authorities relating to importation) without regard to section 202 of the IEEPA (50 U.S.C. 1701) in the case of any commercial activity in the United States by a person that is on the list." Of IEEPA grants the President sweeping powers to prohibit transactions and block property and property interests for nations and other groups subject to an IEEPA national emergency declaration. Consequently, those companies identified by the DOD on a list per Section 1237 could be blocked and prohibited from doing business with U.S. entities and others and those that do business with such Chinese companies could be subject to enforcement actions by the U.S. government (e.g. the U.S.'s actions against ZTE for doing business with Iran in violation of an IEEPA national emergency).

The statute defines a "Communist Chinese military company" as "any person identified in the Defense Intelligence Agency publication numbered VP-1920-271-90, dated September 1990, or PC-1921-57-95, dated October 1995, and any update of those publications for the purposes of this section; and any other person that is owned or controlled by the People's Liberation Army; and is engaged in providing commercial services, manufacturing, producing, or exporting." Considering that the terms "owned" and "controlled" are not spelled out in this section, the executive branch may have very wide latitude in deeming a non-Chinese company as owned or controlled and therefore subject to the President's use of IEEPA powers.

Moreover, since the President already has the authority to declare an emergency and then use IEEPA powers, this language would seem to allow the President to bypass any such declaration and immediately use such powers, except those regarding importation, against any Chinese entities identified on this list by the Pentagon.

Finally, Schumer, Cotton, Gallego, and Gallagher ask Esper

1. When was this list of Communist Chinese military companies operating in the United States last updated by the Department of Defense?
2. As part of your commitment to achieving the goals set out in the 2018 National Defense Strategy, will you commit to updating and publicly releasing this list as soon as possible?

In the other letter, Schumer and Cotton press Federal Communication Commission Chair Ajit Pai on the agency's "legacy authorizations to Chinese state-owned telecommunications companies

operating in the U.S." They noted the May 2019 denial of China Mobile USA's application for authorization to "provide international telecommunications services between the United States and foreign destinations" as explained in the FCC's memorandum and opinion. Schumer and Cotton also noted the FCC's reliance on "Team Telecom," an interagency working group that consists of "national security, law enforcement, and foreign and trade policy experts through the executive branch" who "concluded that China Mobile USA was vulnerable to exploitation, influence, and control by the Chinese government." Team Telecom further concluded that should the FCC authorize China Mobile USA to operate in the U.S., it would present "national security and law enforcement risks that could not be addressed by a mitigation agreement." These experts also raised concerns about the implications of China's 2017 "national intelligence law that requires Chinese companies to support, provide assistance, and cooperate in China's national intelligence network, wherever in the world they operate."

On this basis of the grounds used to deny China Mobile USA's application, Schumer and Cotton requested that the agency revisit the authorizations granted to two other Chinese telecommunications companies: China Telecom and China Unicom. They raised questions about the risks posed by the operation of these two companies in the U.S. to U.S. national security. They asked the FCC to "open a proceeding to review whether [these legacy authorizations for these two companies] continue to serve the public interest and, if necessary, should be revoked."

These letters are the latest in a number sent to the Trump Administration this year. In March, Gallego and Gallagher sent a letter to the Pentagon regarding "Chinese telecommunications firms seeking to construct 5G networks around the world [that] represent a potential threat to American national security and the information security of allies and partners."

There have also been a number of bills introduced that would require the executive branch to take action against the Chinese government and Chinese companies. In January, Gallagher, Gallego, Cotton, and Senator Chris Van Hollen (D-MD) introduced the "Telecommunications Denial Order Enforcement Act" (H.R. 602) that "direct the President to impose denial orders banning the export of U.S. parts and components to Chinese telecommunications companies that are in violation of U.S. export control or sanctions laws" according to a press release. The "Defending America's 5G Future Act" (S. 2118) would "codify President Trump's Executive Order that placed Huawei on the Commerce Department's Entity List and would also provide Congress with the ability to block waivers provided to companies looking to engage in business with Huawei" according to a press release.

50 State AGs Looking Into Google's Antitrust Practices

Last week, 50 state attorneys general announced a joint anti-trust investigation into Google regarding possible violations. The investigation will apparently be led by Texas Attorney General Ken Paxton (R) and Washington D.C. Attorney General Karl Racine (D). In his press release, Paxton announced "a multistate, bipartisan investigation of tech giant Google's business practices in accordance with state and federal antitrust laws…[notably] Google's overarching control of online advertising markets and search traffic that may have led to anticompetitive behavior that harms consumers." He said that "[l]egal experts from each state will work in cooperation with Federal authorities to assess competitive conditions for online services and ensure that Americans have access to free digital markets."

Paxton stated

> Past investigations of Google uncovered violations ranging from advertising illegal drugs in the United States to now three antitrust actions brought by the European Commission. None of these previous investigations, however, fully address the source of Google's sustained market power and the ability to engage in serial and repeated business practices with the intention to protect and maintain that power.

The news of the investigation into Google follows New York Attorney General Leticia James' recent announcement of 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."

In June, a number of media outlets reported that the U.S. Department of Justice (DOJ) and the Federal Trade Commission (FTC) have started investigations into the alleged antitrust activities of Google and Amazon. Most of the articles relied on the statements of three people with "knowledge" of the discussions but who are unauthorized to discuss the deliberations publicly, suggesting senior officials at DOJ and/or the FTC. The announcement came at a time when the agencies are feeling more pressure from Capitol Hill on what are being called anti-competitive and anti-consumer policies of a number of large technology firms, including Facebook and others, from both the right and the left.

The DOJ and FTC have overlapping, interlocking authority to police antitrust and anti-competitive practices granted primarily under three statutes: the Sherman Act (15 U.S.C. §§ 1-7), the Clayton Act (15 U.S.C. §§ 12-27), and the FTC Act (15 U.S.C. §§ 41 et seq.). The agencies have traditionally divided markets based on expertise with the FTC specializing in these matters relating to "health care, pharmaceuticals, professional services, food, energy, and certain high-tech industries like computer technology and Internet services." The agencies often decide which one will tackle a possible antitrust or anti-competitive issue, and according to *Reuters*, DOJ's Antitrust Division and the FTC met a few weeks ago and decided that the former agency would look into Google and Apple while the latter agency would investigate Amazon and Facebook.

The DOJ is said to be interested in Google's practices in its digital advertising business and its Android operating system. However, the DOJ reportedly needed to consult with the FTC regarding the launch of an investigation given the latter agency's recent investigation of Google. During the Obama Administration, the FTC investigated Google and secured a commitment from the company to stop some practices but ultimately did not find evidence supporting an antitrust action.

In late July, Google confirmed the DOJ probe. In its recent 8-K filing with the Securities and Exchange Commission (SEC), Google's parent company, Alphabet explained

> Alphabet Inc. ("Alphabet") previously disclosed in its Form 10-Q filed on July 26, 2019:
>
> > "The online technology industry and our company have received increased regulatory scrutiny in recent months. In July 2019, the Department of Justice (DOJ) announced that it will begin an antitrust review of market-leading online platforms.

> We continue to engage with the DOJ, the EC, and other regulators around the world regarding competition matters."

> On August 30, 2019, Alphabet received a civil investigative demand from the DOJ requesting information and documents relating to our prior antitrust investigations in the United States and elsewhere. We expect to receive in the future similar investigative demands from state attorneys general. We continue to cooperate with the DOJ, federal and state regulators in the United States, and other regulators around the world.

Additionally, it appears that the FTC's antitrust division is also investigating Amazon's share of the retail market. Reportedly, a number of merchants have recently received investigative requests from the FTC on Amazon. And, the retail giant is also facing anti-trust scrutiny in Europe, too. In July, the European Union announced the opening of "a formal antitrust investigation to assess whether Amazon's use of sensitive data from independent retailers who sell on its marketplace is in breach of EU competition rules."

Joint Committee Hearing On "Securing the Nation's Internet Architecture"

On September 10, two subcommittee held a hearing "on how departments and agencies across the federal government coordinate to secure the critical components and locations upon which the nation's internet architecture depends" according to a committee memorandum.

The House Armed Services/Intelligence and Emerging Threats and Capabilities and House Oversight & Reform/National Security Subcommittees heard from

- The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's Assistant Director for Cybersecurity Jeanette Manfra
- Acting Assistant Secretary of Commerce and National Telecommunications and Information Administration Administrator Diane Rinaldo
- Deputy Assistant Secretary of Defense for Cyber Policy Ed Wilson

Intelligence and Emerging Threats and Capabilities Chair Jim Langevin (D-RI) said the subcommittees were conducting much needed oversight regarding the security of the internet's underlying architecture, namely the components, physical sites, and the assets that are necessary for the internet to operate. He said that defending the U.S.'s assets in this global telecommunications networks requires a whole of government approach, and he expressed concern that the federal government is not approaching the subject in a cohesive or comprehensive manner, creating significant risk for the nation. Langevin noted that both subcommittees are seeking a better understanding of statutes, policies, and guidance, and inter-agency agreements that govern this critical internet architecture. He stated that the subcommittees are interested in any gaps and whether legislative solutions may be needed. Langevin stated that despite most people not understanding the broader picture regarding the internet's structure, the larger architecture allows for the world to flow into people's hands. He added that this architecture include the high capacity cables buried below the ground and laid below the sea and the cable landing stations that connect the cables from continent to continent. Langevin noted the internet exchange points that serve as clearinghouses for data between internet service providers and content delivery networks. These physical sites and tangible items, Langevin said, are necessary for the internet to operate effectively. He said these are viewed as distinct from the networks, protocols, and software that most people understand as the internet. He remarked that unplugging a network cable was just as effective as a denial of service attack and maybe more so. Langevin said that it is difficult for the

federal government to attack the problems presented by the internet architecture because of the departments' overlapping jurisdiction, responsibilities, and capabilities. He expressed his concern that the federal government has fragmented internet architecture security among multiple departments as opposed to conceptualizing the internet ecosystem as a whole with departments working collaboratively. Langevin said the Department of Homeland Security serves as the lead for all critical infrastructure and the sector-specific agency for the telecommunications sector, and yet the Department of Commerce's National Telecommunications and Information Administration is principally responsible for advising the President on telecommunications and information policy issues. He stated that the NTIA also develops national policy on internet and cybersecurity issues. Langevin stated that the Department of Defense is broadly responsible for defense of the nation, and other agencies have responsibilities in this realm, notably the Federal Communications Commission. He said he does not doubt these agencies work together, but he expressed his worry that by carving out distinct policy lanes, agencies are missing some issues such as internet architecture security. He said he was interested in hearing about engagement with the private sector and how agencies address the fact that internet architecture is neither purely a cybersecurity nor a physical security problem.

Intelligence and Emerging Threats and Capabilities Ranking Member Elise Stefanik (R-NY) said as the subcommittees consider the security of the internet architecture, members should remind themselves of the urgency of the task. She said firstly, the enormity of the physical challenges are worth mentioning. Stefanik that the world's internet architecture and the U.S.'s domestic architecture are highly integrated with varying levels of resiliency and redundancy. She remarked that in some cases there are international norms even though laws and policies often vary by country and by sector. Stefanik said there are many points of failure and it remains so contested and complex that risk managers lack full awareness on how to identify and mitigate threats or weaknesses. Stefanik stated, secondly, the Intelligence Community provides sobering assessments on adversarial use and exploitation of the internet, and in the most recent Worldwide Threat Assessment stated "our adversaries and strategic competitors will increasingly use cyber capabilities including cyber espionage, attack and influence operations to seek political, economic, and military advantage over the U.S., its allies, and partners." Stefanik said that the physical internet architecture is the highway upon which these adversaries travel. She asserted that our adversaries understand U.S. vulnerabilities and will not hesitate to exploit these weaknesses to further their strategic and economic objectives. She declared that the U.S. is no longer peerless and security is not assured. Stefanik said that Russia and China are adapting to and learning from U.S. weaknesses by building what amounts to their state-owned internet architecture to monitor, control, and influence their own populations. She said these controls will make it harder for the U.S. to exercise strategic, political, and military options. Stefanik articulated her concern that the U.S. does not have a holistic strategy to mitigate and respond to these nations. She acknowledged that while agencies are cooperating more, much work remains to be done.

National Security Chair Stephen Lynch (D-MA) remarked that the hearing would focus on how federal agencies work to protect the critical architecture upon which the internet and telecommunications depend. He said the subcommittees hope to work together to identify gaps and needs across the agencies to better defend the internet architecture. Lynch noted that interrupted and consistent access to the internet is critical for daily life in the 21st Century as citizens need the internet to be fully integrated into the economy and businesses through the U.S. need access in order to participate in the national and international economies. He stated that the U.S. military needs internet access to conduct operations and is tasked with protecting the nation from malicious cyber actors. He added that the internet is crucial for helping areas develop economically. Lynch said that

given the growing reliance on the internet in the U.S. has made temporary interruptions in service a source of serious and cascading effects across the nation's critical infrastructure. He noted that no single U.S. entity is responsible for securing the internet and its underlying architecture. Lynch said instead the U.S. has multiple agencies with varying jurisdictions and roles and adding to this complexity is the fact the private sector mostly owns the fiberoptic cables, data centers, and undersea cables that constitute the internet's architecture. He contended that as a consequence, communication and coordination across the public and private sector are crucial but claimed the challenge the U.S. faces is that "when everyone's in charge, no one's in charge." Lynch added that the physical architecture of the internet is susceptible to natural disasters, human accidents, and intentional actions by sophisticated malign actors. He quoted the 2019 Worldwide Threats report's assessment that Russia has been mapping U.S. cyber infrastructure with an eye to knocking out key portions if necessary. Lynch said multiple open source reports have noted the increase in military activity near undersea cables, suggesting planning to allow for just such an occurrence in the event of hostilities or war.

National Security Ranking Member Jody Hice (R-GA) noted that the hearing topic may not be the "flashiest" but it is among the most important. He said he wanted the witnesses to discuss a whole of government approach and how to move the federal government towards that strategy. Hice said this is an urgent topic the Congress needs to address head on.

Manfra said that "[t]he challenge of effectively coordinating homeland security and homeland defense missions is not new, but it is amplified and complicated by the global, borderless, interconnected nature of cyberspace where strategic threats can manifest in the homeland without advanced warning." He stated that "[a]lmost a year ago, Department of Homeland Security (DHS) and the Department of Defense (DOD) finalized an agreement, which reflects the commitment of both Departments in collaborating to improve the protection and defense of the U.S. homeland from strategic cyber threats." Manfra said that "[t]his agreement clarifies roles and responsibilities between DOD and DHS to enhance U.S. government readiness to respond to cyber threats and establish coordinated lines of efforts to secure, protect, and defend the homeland."

Manfra said that "DHS and DOD are both committed to improving the protection and defense of the homeland from strategic cyber threats." Manfra stated that "[s]pecifically, DHS and DOD are working

- to improve intelligence, indications, and warning of malicious cyber activity;
- strengthen the resilience of the highest priority national critical infrastructure;
- improve joint operations planning and coordination;
- improve joint incident response to significant cyber incidents;
- expand cooperation with State, local, tribal and territorial authorities; and
- improve joint defense of Federal networks.

Manfra claimed that "DHS and DOD will achieve these objectives through three primary lines of effort:

- First, DOD and DHS are adopting a threat-informed, risk-based approach that ensures the resilient delivery of national critical functions and services, and denies strategic adversaries the ability to prevent delivery of such functions and services. DOD and DHS will jointly prioritize a set of high priority national critical functions and non-DOD owned mission critical infrastructure that is most critical to the military's ability to fight and win wars and project power.

- Second, DOD and DHS, in coordination with the FBI and the intelligence community, are collaborating to build a common understanding of strategic cyber threats that can empower private sector network defenders, critical infrastructure owners and operators, and government actors to improve resilience and integrity of national critical functions. Timely access to threat information related to adversary capabilities and intent is critical to understand and counter the risk facing our nation's critical infrastructure effectively.
- Third, DOD and DHS are coordinating to inform and mutually support respective planning and operational activities as appropriate for each Department's unique authorities. DHS's knowledge of the domestic risk landscape, its work with the private sector, can inform DOD's efforts to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure. And, DOD's "defend forward" operations can inform and guide DHS efforts to anticipate adversary action and understand potential risks to critical infrastructure.

Manfra noted "[a]n unclassified joint paper released in 2017 by DHS and the Office of the Director of National Intelligence – in coordination with the private sector – examined the risks to undersea cables and landing stations and potential avenues to mitigate such risks." She stated that "[u]ndersea cables transmit more than 97 percent of the world's electronic communications and pose potentially devastating consequences in the event of failure. In addition to accidental physical threats, there are vulnerabilities relating to nation-state adversaries, cyberterrorists, hactivitists, and cybercriminals."

Rinaldo said that "[t]he Nation's telecommunications infrastructure is the physical medium through which all Internet traffic flows…[and] underpins the foundation of our digital economy." She stated that "NTIA's role is to foster national safety and security, economic prosperity, and the delivery of critical public services through telecommunications." Rinaldo stated that "[i]n this capacity, NTIA is involved in numerous policy issues that affect the security of critical elements of our Nation's telecommunications infrastructure, encompassing exchange points, data centers, content delivery networks, the domain name system, undersea cables, and cable landing stations, as well as the diverse array of communications access networks and technologies that enable American consumers, businesses, and other institutions to connect to the Internet." He said that "[o]ur support includes working with our interagency partners to enhance the security of our Nation's telecommunications supply chain, advocating the United States' longstanding policy against data localization regimes, and participating in Executive Branch reviews of applications before the FCC that involve transactions with a significant foreign ownership component." Rinaldo added that "[w]e also are supporting the Secretary of Commerce as needed on the implementation of the Executive Order on Securing the Information and Communications Technology and Services Supply Chain."

Wilson said that the "DOD relies heavily upon the global internet architecture including internet exchange points, data centers, content delivery networks, undersea cables, international telecommunications, and related infrastructure. Undersea cable systems are vital to the execution of DOD's missions globally." He stated that "[t]he Department has been leasing bandwidth on privately owned undersea cable systems since the 1980s." Wilson explained that "DOD prioritizes mission-essential traffic and the Defense Information Systems Agency (DISA) is constantly working with the Combatant Commands, Military Departments, and Defense Agencies to meet mission requirements." He contended that "[t]he U.S. Government has a limited and specific role to play in defending against attacks on our Nation's internet architecture, including through DOD's trusted relationships with industry."

Wilson said that "[s]ecurity was not a major consideration when the Internet was designed and fielded." Wilson said that "[a]lthough computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control, the private sector owns and operates well over ninety percent of all of the interdependent networks of information technology infrastructures across the cyber domain." He remarked that "[a]t the same time, the Nation's telecommunications infrastructure is primarily owned by commercial entities." He explained that "[o]ur adversaries target our Nation's weakest links, and vulnerabilities are consistently found across the full scope of the Internet ecosystem be it government or industry targets." Wilson said that "[t]he Department, which views the challenges it faces in performance of its critical missions principally through a national security lens is nonetheless highly dependent on privately-owned infrastructure, decisions concerning which are regularly guided by ordinary business – or economic – considerations." HE stated that "[r]ecognizing this inherent tension, defending national critical infrastructure, including the Nation's internet architecture, from significant foreign malicious cyber activity has become an area of increased emphasis for the Department."

Senate Homeland Security Delves Into Cybersecurity As Part of Its 9/11 Anniversary Hearing

On September 9, the Senate Homeland Security and Governmental Affairs Committee held a field hearing in New York City titled "18 Years Later: The State of Homeland Security after 9/11" at which U.S. cybersecurity was one of the main topics discussed.

In his opening statement, Chairman Ron Johnson (R-WI) remarked that "[t]he [Bipartisan Policy Center's] 10th Anniversary Report Card showed significant implementation of the 41 recommendations, but those were solutions in response to 9/11." He stated that "[i]n 2015, this Committee's then Ranking Member issued a report reviewing the department of homeland security…[and] [h]e detailed $541 million spent by DHS from 2003 to 2014 and criticized the department for not successfully executing any of its five main missions…prevent terrorism, enhance security, secure and manage our borders, and worse and administer immigration laws, safeguard and secure cyberspace, strengthened national preparedness and resilience." Johnson said that "I hope that we can fairly evaluate past successes and failures and use these assessments to guide future actions and policies designed to secure our homeland."

Ranking Member Gary Peters (D-MI) stated that "[t]oday, DHS confronts a new generation of persistent and evolving threats, more complex and diffuse than we could have imagined just a few years ago." He said that "[w]ith each passing day, our world becomes more interconnected, cementing the important role cybersecurity plays in our everyday lives." Peters asserted that "[t]he Department of Homeland Security is our first line of defense against these and many other challenges, some of which have evolved or risen since this department was created." He said that "[a]s the threats to our homeland change, so must the efforts to protect our national security…[and] [w]ith nearly two decades of lessons learned, the time has come for a clear-eyed assessment of what has worked and what needs to be improved." Peters stated that "[i]n order to build a more sustainable department and defend ourselves from global threats, we must look to the future…[and] also ensure that DHS is prepared to anticipate and identify those threats arising in the future."

Former Secretary of Homeland Security Michael Chertoff stated that "there are a number of areas of activity [in cybersecurity] that I would highlight as vital to allowing us to address the most pressing threats.

- First, in the area of election security, the work of DHS' Cyber and Infrastructure Security Agency or CISA is making progress in helping to enhance cyber and physical infrastructure security. In particular when it comes to election security, CISA has helped provide information to state and local election officials to help them defend their infrastructure and partnered to share cybersecurity risk information and we see action being taken. In 2016, less than 30% of election infrastructure was protected by intrusion detection systems. By the last midterms, coverage was up to 90%. This is a great accomplishment, but more must be done. We need to allocate more money and resources for CISA to continue its mission and work with states and localities in need of further assistance. We also need to act to deter foreign adversaries from trying to affect our elections.
- Second, I believe that we need to foster growth within the National Technology Industrial Base. During the Cold War, the Defense Industrial Act was effective at maintaining the United States' industrial advantage, but now its limitations are starting to show. Globalization has made the production of certain technologies—computer chips for instance—prohibitively expensive in the United States. While Congress' amendment to the Defense Industrial Act to include dual-use technologies was a step in the right direction, there is still much to be done. We must "recognize these changed circumstances and then reconstruct legal and policy standards."
- Third, supply chain vulnerabilities, both digital and physical are of increasing concern. The U.S. government must continue to prohibit federal agencies from using hardware and software from companies that pose a national security risk. The U.S. government has already done this with the prohibitions of Russia's Kaspersky and China's Huawei. We must continue to take action to protect our critical infrastructure supply chain. Our electrical grid, banking system, and water supply are critical aspects of our economic and national security, and their vulnerabilities must be secured.
- Fourth, the U.S. government must focus on cultivating its relationship with our allies and with the private sector, which plays a paramount role in the National Technology Industrial Base. We have entered an era where nearly every technology we encounter is effectively "dual-use," that is, a technology that has civilian, government, and military applications. DHS, the intelligence community, and the Department of Defense are all reliant on technologies developed in the private sector and supply chains that provide equipment to both the commercial sector and government. In this environment it is paramount that our leaders work closely with leading American technology companies, working to ensure that their products remain cutting edge and have the security needed to be used in our homes, businesses, power plants, and government buildings.

Former Secretary of Homeland Security Janet Napolitano said that "I am here today to address three future threats that the Department can and must confront. They are: cyber security, mass casualty shootings, and climate change." She said "[d]uring his tenure, Secretary Johnson did a remarkable job of bolstering DHS's cyber capabilities, and I applaud Congress for working with the department to transform the National Protection and Programs Directorate into an operational agency, the Cybersecurity and Infrastructure Security Agency." Napolitano stated that "we have much more to do in this area." She declared that "[o]ur nation's critical infrastructure, its utility grids, election systems, and our public and private networks are all vulnerable." Napolitano stated that "[o]ur adversaries and international criminal organizations have become more determined and more brazen in their efforts to attack us and to steal from us." Napolitano said that "[w]e need a whole of government and a whole of public and private sector response to this threat, and it needs to happen immediately." She said that "[o]ur public research universities and the Department of Energy national labs are tremendous resources and incredible partners for DHS in working to

address the real challenges before us…[and] [w]e can all do more to build partnerships and invest in our nation's research enterprise that is critical to protecting our national security."

Former Secretary of Homeland Security Jeh Johnson stated that "[w]ithout a doubt, Russian interference in the 2016 election highlighted a new form of cyber threat." He said that "[t]he hacks into the DNC represented not just a cybertheft, but a weaponization of that stolen material for purposes of foreign influence on voter attitudes…[and] [t]he scanning, probing and infiltration of voter registration data highlighted the vulnerability of state election systems." Johnson said that "[t]he masked foreign dissemination of fake news and extremist views in the U.S. revealed that our strength as an open society is also our vulnerability." Johnson stated that "[f]ollowing my January 2017 designation of election infrastructure in this country as critical infrastructure, it appears DHS has been working effectively with state election officials to improve their cybersecurity." He declared that "[t]his is good news."

Johnson remarked that "[t]hough I am not in a position to endorse specific legislation, I generally support federal legislation to further assist states in their election cybersecurity efforts." He asserted that "[i]ntelligence reports indicate that Russian efforts to influence our democracy continue unabated." Johnson stated "[t]here can be no complete line of defense against such activity; it is therefore up to the U.S. government, the current Administration, and the current President to impose costs for cyberattacks by nation-states sufficient to serve as deterrents." He contended that "[a]ll nation-states –whether democracies, monarchies, or communist regimes –respond to sufficient deterrents that render bad behavior cost prohibitive." He said that "[w]hen it comes to Russian efforts to interfere in our democracy, it appears that our government has yet to impose those appropriate costs." Johnson stated that "[t]hough Congress and the Trump Administration have imposed considerable sanctions on the Russians, and President Trump's subordinates sound dire alarms that "our democracy itself is in the crosshairs, "the President himself appears to not take the threat seriously, barely acknowledges it exists, and has yet to communicate directly to President Putin in any serious way that the U.S. will not stand for it any further."

GAO Rates Army's Cyber and Electronic Warfare Initiative

The Government Accountability Office (GAO) released its most recent assessment of the Army's initiative to reorient its operational mission to incorporate cyber to a greater degree (i.e. The U.S. Army in Multi-Domain Operations 2028.) These plans are changing the organization, missions, and procurement of the Army, particularly in the cyber and electronic warfare realms. In "FUTURE WARFARE Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations," the GAO made "three recommendations, including that the Army comprehensively assess the risk of staffing, equipping, and training the cyber and electronic warfare units that it has activated at an accelerated pace, and to do so for new organizations it plans to activate in an accelerated manner for multi-domain operations."

The GAO performed this assessment because of language in the House Armed Services Committee's committee report for FY 2018 National Defense Authorization Act for Fiscal Year 2018 that tasked the GAO with reviewing "the Army's progress in implementing the new warfighting concept." The GAO explained that "[t]his report addresses

> (1) how the Army is changing its doctrine, organizations, and training in order to execute multi-domain operations;

> (2) the extent to which the Army has established new cyber and electronic warfare units, including any challenges faced by these units, and whether the Army assessed risks associated with its plan to establish these units; and
> (3) how the Army has engaged with the Joint Staff and other services to develop its new warfighting concept."

In terms of background, the GAO explained that "the Army has been developing a new Army Operating Concept, which the Army is using to define how its forces will engage jointly with the other services for the task of deterring and defeating Chinese and Russian aggression in both competition and conflict." The GAO stated that "[t]he Army calls this concept The U.S. Army in Multi-Domain Operations 2028, and it would enable the Army to confront adversaries in contested environments by presenting those adversaries with multiple challenges across multiple domains (land, air, sea, cyber, and space)." The GAO stated that "[t]he multi-domain operations concept will significantly affect Army doctrine, organizations, and training in the coming years."

The Defense Intelligence Agency (DIA) has recently assessed both Russia and China's military capabilities. In its June 2017 report titled "RUSSIA MILITARY POWER: Building a Military to Support Great Power Aspirations," the DIA stated

> Russia views the information sphere as a key domain for modern military conflict. Moscow perceives the information domain as strategically decisive and critically important to control its domestic populace and influence adversary states. Information warfare is a key means of achieving its ambitions of becoming a dominant player on the world stage. Since at least 2010, the Russian military has prioritized the development of forces and means for what it terms "information confrontation," which is a holistic concept for ensuring information superiority, during peacetime and wartime. This concept includes control of the information content as well as the technical means for disseminating that content. Cyber operations are part of Russia's attempts to control the information environment.

Earlier this year, the DIA asserted in its report "CHINA MILITARY POWER: Modernizing a Force to Fight and Win,"

> Authoritative People's Liberation Army (PLA) writings identify con-trolling the "information domain"—sometimes referred to as "information dominance"—as a prerequisite for achieving victory in a modern war and as essential for countering outside intervention in a conflict. The PLA's broader concept of the information domain and of information operations encompasses the network, electromagnetic, psychological, and intelligence domains, with the "network domain" and corresponding "network warfare" roughly analogous to the current U.S. concept of the cyber domain and cyberwarfare. The PLA Strategic Support Force (SSF) may be the first step in the development of a cyber-force by combining cyber reconnaissance, cyberattack, and cyberdefense capabilities into one organization to reduce bureaucratic hurdles and centralize command and control of PLA cyber units. Official pronouncements offer limited details on the organization's makeup or mission.

The GAO added that

> we also reported in January 2019 that establishing the Army Futures Command creates unique opportunities for the Army to improve its modernization efforts and that the Army

has generally applied leading management practices, such as well-defined team goals and senior management support, to its modernization. However, we also reported that the Army may be beginning weapon systems development before technology is sufficiently mature. This raises the risk that the resulting systems could experience cost increases, delivery delays, or failure to deliver desired capabilities.

The GAO asserted that "[t]he refinement of the Army's Operating Concept is beginning to drive changes across the Army...[and] is making near-term changes by incorporating multi-domain operations into its doctrine, organizations, and training, which includes the accelerated creation of new cyber and electronic warfare units." The GAO noted "these units are short of both people and equipment." The GAO stated that "[t]he Army plans to incorporate this unit into the first Multi-Domain Task Force by the end of Fiscal Year 2020, but in the meantime the unit could be deployed if needed." The GAO noted that "[t]he Army did prepare a preliminary risk assessment for the 915th Cyber Warfare Support Battalion prior to activation, but it is unclear whether the Army will perform a more comprehensive risk assessment as the unit matures and nears full operational capability." The GAO stated that "[f]or the units already activated, a risk assessment could benefit the Army by providing insights about the ability to deploy and sustain the units...[and] [i]t is important for the Army to assess its efforts before committing resources to activate new units." The GAO stated that "[b]y formally assessing the risk of all new units activated in an accelerated manner, the Army will have the key information its leaders need for making decisions related to the activation of those units and other related units going forward."

Going forward, the House Armed Services Committee could fold language into a future NDAA or committee report directing the Army to fulfill the GAO's recommendations or others on the Army's efforts to reorient their planning through the incorporation of cyber and electronic warfare.

Other Hearings

- House Energy & Commerce/Communications & Technology – "Legislating to Connect America: Improving the Nation's Broadband Maps."
- House Homeland Security – "Global Terrorism: Threats to the Homeland, Part I"
- House Financial Services/Task Force on Artificial Intelligence – "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities"
- **POSTPONED:** House Judiciary/ Antitrust, Commercial and Administrative Law – "Online Platforms and Market Power, Part 3: The Role of Data and Privacy in Competition"

Further Reading

- "YouTube creators have begun shifting channels after FTC fine leaves futures in jeopardy" – *The Verge*. In light of the Federal Trade Commission's COPPA settlement with Google and YouTube, many content creators on the social media platform are trying to adapt to the new requirements not to collect data from nor target children.
- "Want to Do Business in Silicon Valley? Better Act Nice" – *The New York Times*. A venture capitalist's frank criticism of a Mark Zuckerberg-led education start up on Twitter was not well received in Silicon Valley, to put matters politely. An interesting look inside the culture of the technology world.
- "Key lawmaker in California Privacy Act debate is married to Ring executive" – *Politico*. AB 873 has been characterized as an attempt to gut the California Consumer Privacy Act. Assemblywoman Jacqui Irwin's (D) support of AB 873 is now being questioned now that the

media has started asking about conflicts of interest considering her husband is the CEO of Ring, "a home security and video doorbell startup that Amazon acquired last year for about $1 billion."

- "Israel accused of planting mysterious spy devices near the White House" – *Politico*. Former U.S. intelligence officials said that Israel's use of devices to capture cell phone call details near the White House and around Washington went unpunished by the Trump Administration. Reportedly, the target were President Donald Trump and his advisors. This article was likely leaked by current U.S. intelligence officials, so make of that what you will.
- "The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once" – *ProPublica*. Hackers are targeting managed service providers, entities to whom many local governments and small and medium sized businesses have outsourced their IT. If these entities have any scale, a successful attempt allows hackers to penetrate a number of entities at the same time. The downside to aggregating the "crown jewels" of multiple entities on the same network or system.
- "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction" – *WIRED*. A new theory from a security firm posits that the hour-long blackout Russian hackers inflicted on Ukraine in 2016 was intended to damage the country's electric grid for months but this plan went awry.
- "Google Says a Change in Its Algorithm Will Highlight 'Original Reporting'" – *The New York Times*. Google will now try to highlight the media outlet that first breaks a story instead of the other outlets that leverage a site's original reporting for page views. Google's announcement comes amidst calls for anti-trust regulators and other stakeholders because of the effect the search engine giant and Facebook are having on the media.
- "Report reveals play-by-play of first U.S. grid cyberattack" – *E&E News*. The North American Electric Reliability Corporation (NERC) detailed the first of its kind cyberattack of the U.S. electric utility left several grid operators effectively blind for five minutes. In a NERC document, the agency explained "A vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices."
- "How Top-Valued Microsoft Has Avoided the Big Tech Backlash" – *The New York Times*. The most valuable tech company on the planet has not been entangled in international, federal, and state efforts to regulate privacy and to address antitrust issues. Why? Partly because of lessons learned during its antitrust investigation and settlement nearly 20 years ago, partly its business model, and partly savvy leadership.
- "Microsoft's president chides Facebook, urges new approaches to combat weaponization of tech" – *The Washington Post*. Microsoft President Brad Smith co-wrote a book, "Tools and Weapons: The Promise and The Peril of The Digital Age," that both details his proposed solutions to a number of tech-related problems like privacy and cybercrime while also calling out rival companies. In this piece, Smith discusses the internal changes at Microsoft after the U.S.'s antitrust investigation in the 1990's that has allowed the company to navigate the current regulatory climate.