Technology Policy Update
19 December 2019
By Michael Kans, Esq.

Senate Encryption Hearing

The Senate Judiciary Committee held a hearing titled "Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy" and there was agreement on both sides of the aisle that the default encryption in devices like iPhones and apps like WhatsApp is posing unacceptable costs on law enforcement and the victims of crimes. There were multiple warnings from Members that unless technology companies do not do more to work with law enforcement agencies to increase access to encrypted devices and communications, Congress would pass legislation to force such cooperation.

Chair Lindsey Graham (R-SC) stated the hearing would examine the problems associated with encryption of social media devices, phones, and how to strike a balance. He declared "the point for me is I appreciate the fact that people cannot hack into my phone, listen to my phone calls, follow the messages, the texts I receive, and how I use the phone." Graham added that "I think all of us want devices that protect our privacy." He stated, "having said that, no American should want a device that becomes a safe haven for criminality." Graham claimed "we're not the only people who use these devices" and "criminals use these devices, terrorists use these devices" and "you've got encrypted apps out there that child molesters use." He asserted "you've got encrypted apps like WhatsApp and Messenger that terrorists use, so here's the deal for me: I want the average American to be protected as much as possible but when law enforcement believes a crime has been committed or it looks like it is in the process of being committed and they get a court order, I want the government to be able to look and find all relevant information." Graham contended there is place safer, more sacred in American politics and legal systems than one's home, and one is king or queen of his or her castle. He said that if the government gets a search warrant, however, to enter a person's home, it can, and if one locks the door, the government can break down the door. Graham claimed in American law, there is no place that is immune from inquiry if criminality is involved. He declared that "I'm not about to create a safe haven for criminals where they can plan their misdeeds and store information in a fashion, they could never access it is a bridge too far for me." Graham conceded he does not know how this would be done, and he hopes the tech community working with law enforcement can find a way to do it. He added that "if you all don't, we will."

Ranking Member Dianne Feinstein (D-CA) stated that "[t]oday's hearing provides an opportunity to examine how technology companies and law enforcement can work together to obtain encrypted information that is vital to investigating and prosecuting serious crimes while protecting people's privacy." She said that "[e]ncryption technology is a very important part of maintaining security and personal privacy…[and]…protects personal information by using a scrambled code and allows users to send sensitive financial or other information over the internet." Feinstein claimed that "[a]t the same time, it is equally important to acknowledge that law enforcement has historically been able, under strict legal requirements, to intercept and obtain communications in order to investigate crimes."

Feinstein said that "[t]his issue really came to the forefront following the shooting in San Bernardino, California, on December 2, 2015…[and] [f]ourteen people lost their lives that day, and 22 more were injured…[b]ut a cellphone was found at the scene of the crime." She stated that "[a]s part of

the investigation, the Federal Bureau of Investigation was unable to unlock it…[a]nd despite a lawful court order, the phone's manufacturer refused to assist law enforcement in unlocking the phone." Feinstein said that "[l]uckily, the FBI was ultimately able to unlock the phone, but that easily could have ended up not happening, and the investigation would have been halted there." She claimed that "[t]he incident showed the importance of bringing technology companies and law enforcement together in order to find ways to cooperate for our safety." Feinstein explained that "[t]hat is why, in 2016, I announced legislation to address this issue…[and] [w]hile I chose not to introduce that legislation, I still believe Congress should be considering ways to address this problem."

Feinstein remarked that "[m]ore recently, the *New York Times* published an article titled: "The Internet is Overrun With Images of Child Sexual Abuse. What Went Wrong?...[that] explains that "increasingly, criminals are using advanced technologies like encryption to stay ahead of the police." She stated that "[t]hese developments concern me a great deal…[and] I hope our witnesses today will address how we can help law enforcement and technology companies stop this terrible trend before it gets worse."

Feinstein stated that "I understand that technology companies are worried that providing access to encrypted information may create unintended weaknesses that hackers could exploit." She explained that "[i]t would be helpful if our witnesses today could identify ways technology could comply with the legal process without creating unacceptable security vulnerabilities." Feinstein declared that "[e]veryone agrees that having the ability to safeguard our personal data is important…[and] [a]t the same time, we've seen criminals increasingly use technology, including encryption, in an effort to evade prosecution." She stated that "[w]e cannot let that happen…[and] [i]t is important that all criminals, whether foreign or domestic, be brought to justice."

New York County District Attorney Cyrus R. Vance, Jr. said "[t]he single most important criminal justice challenge in the last ten years is, in my opinion, the use of mobile devices by bad actors to plan, execute, and communicate about crimes." He said that "[j]ust as ordinary citizens rely on digital communication, so do people involved in terrorism, cyber fraud, murder, rape, robbery, and child sexual assault." Vance claimed that "[f]or this reason, lawful, court-ordered access to these communications has become essential for us to prevent crime, to hold people accused of crimes accountable, and to exonerate the innocent." He asserted that "[u]ntil the fall of 2014, Apple and Google routinely provided law enforcement access to their mobile phones when they received a court-ordered search warrant…[but] [t]hat changed when they rolled out their first mobile operating systems that, by design, often make the contents of smartphones completely inaccessible." Vance contended that "[i]n doing so, Apple and Google effectively upended centuries of American jurisprudence holding that nobody's property is beyond the reach of a court-ordered search warrant."

Vance claimed that "Apple and Google, meanwhile, have framed this issue as an either/or proposition: either we can have user privacy or lawful access, but we can't have both, they say." He stated that "they've been successful in propagating this message, even though it's not true." Vance claimed that "My Office is not anti-encryption…[but] [t]hat does not mean encrypted material should be beyond the law when a judge signs a search warrant – especially when we're talking about evidence tied to a child sex abuse case or a potential terrorist attack." He argued that "Apple and Google have maintained their absolutist position that no form of lawful access can be reconciled with privacy concerns…[and] [y]et they have not demonstrated to law enforcement leaders what, if any, damaging effects to user privacy their pre-2014 cooperation with law

enforcement caused." He asserted that "[f]urther, they have decided for their own private business interests that the Fourth Amendment grants a right, not just to privacy, but to anonymity." Vance argued that "[t]his is wrong, and it upends the careful balance our Constitution strikes between privacy and public safety interests."

Vance stated that "[t]o be clear, I, as well as prosecutors across America, are not asking Apple or Google for something extraordinary…[and] [w]e are not asking for a "backdoor" mechanism that would allow our offices to surreptitiously snoop on private citizens…[n]or do we want "surveillance" of smartphone communications." He stated that "[i]nstead, we are asking these companies to comply with warrants issued by impartial judges upon findings of probable cause: something I explained in letters to Apple CEO Tim Cook and Google CEO Larry Page in 2014." Vance claimed that "[a] middle ground exists in the smartphone encryption debate…[and] [t]he right balance between privacy and public safety can be achieved by (1) requiring a court-ordered search warrant, and (2) limiting the information sought to data at rest (for example, the photos and messages that are already on your phone)…[i]n other words, I'm not talking about surveillance of live discussions or other communications while they are in progress."

University of Texas Professor Matt Tait said that "[e]ncryption makes us undoubtedly safer online from hackers and foreign government surveillance…[and] [w]ithout it, the Internet would not be the thriving hub of commerce that it is today." He stated that "[e]ncryption has made it possible to communicate securely with one another, to build businesses online, and enables us to access global communities and shared interests that previously were hard to access." Tait stated that "[t]he Internet and the technology market today is as it is precisely because encryption enables us to operate online securely." He said that "[a]s with all technologies, encryption comes with inevitable collateral externalities, in this case to law-enforcement." Tait remarked that "[i]t is right that we ask hard questions about what we can do to mitigate these collaterals without undermining the huge benefits to society that encryption gives us all." Tait stated that "[w]e should not be coy: encryption does affect law-enforcement in practically all domains, from counter-terrorism, financial crimes, countering child abuse, as well as ordinary device searches for local law-enforcement…[a]nd given the sheer scale and complexity of these domains, it is hardly surprising that the conversation around encryption needs some work itself to decipher."

Tait claimed that "the use of zero-day vulnerabilities has, in effect, become the accepted default mechanism for law-enforcement and intelligence agencies to conduct wiretaps on end-to-end encrypted platforms." He said that "[a] few months ago, a recent hacking campaign attributed to China made use of iPhone zero-day vulnerabilities to access, among other things, the content of WhatsApp and iMessage communications from targeted devices." Tait conceded that "[z]ero-day vulnerabilities are not cheap, but at least for now, wiretaps via hacking remain an attractive, practical, and proportionate method for federal law-enforcement to conduct wiretaps without the need for proactive regulation or help from technology vendors." He stated that "[t]he so-called "cyber-tips" are a harder challenge to bridge." He asserted that "[h]ere the use of zero-day vulnerabilities to break into substantively all devices and scan for abuse material would clearly not be safe or proportionate…[b]ut other approaches do exist that do not require the alteration or removal of end-to-end encryption." Tait stated that "[f]or example, technology vendors can scan for abuse images as they are sent and received on the device itself rather than as it traverses the communications platform."

Tait stated that "[i]n short, options exist for both conducting wiretaps and retaining "cyber tips" without the need for altering or regulating end-to-end encryption. These options are not easy, to

be sure, but they exist." He said that "[u]niquely among the problem domains, only device encryption, which thwarts device searches, would be amenable to a "front door" access mechanism." Tait stated that "[t]his is because device searches can be predicated on the knowledge, if not consent, of the owner, and the technology to do so can be built around law-enforcement's physical access to the device." Tait stated that "[b]ecause these factors are not available in the context of wiretaps, it will always be dangerous to extrapolate technological access mechanisms for device searches to wiretaps or end-to-end encryption generally." He stated that "[i]n summary, encryption remains an important tool for enabling the Internet to operate as the hub of commerce and communication that is increasingly the center of all our lives…[but] [t]here are collateral externalities to law-enforcement investigations, but many of these externalities can be mitigated entirely without reference to the encryption itself."

Apple Manager of User Privacy Erik Neuenschwander asserted that "[e]ncryption not only protects a person's sensitive data, it is also one of the most important mechanisms we have as a nation to safeguard an increasingly interconnected future." He stated that "[e]very day, over a trillion transactions—from financial transactions to the exchange of healthcare records—occur safely over the Internet because of encrypted communications." Neuenschwander stated that "[u]tilizing 5G networks, connected devices will play an even larger role in the operation and maintenance of our critical infrastructure, running our electric grids, transportation networks, and healthcare and financial systems." He contended that "[e]ncryption is needed to protect from malicious actors whose attacks are growing exponentially in scope, frequency, and sophistication…[a]nd encryption will become even more important as more devices are added to the Internet and attack surfaces expand."

Neuenschwander claimed that "[e]ncryption is woven through our software, hardware, and services for maximum security…[and] [w]e also challenge ourselves to collect as little customer data as possible, including through the use of tools that process data only on a person's device, rather than on Apple's servers; if we don't have your information, then nefarious insiders or malicious hackers who gain access to Apple's networks won't either." He contended that "our use of Secure Enclave, a hardware-based key manager that is isolated from the main processor, provides an extra layer of security…[and] [o]verall, our approach to design improves security, reducing points of vulnerability and risk."

Neuenschwander explained that "[w]e understand that rapidly evolving technologies, by their very nature, can create challenges for investigators…[and] [a]t Apple, we share law enforcement's goal of creating a safer world, and we work closely with law enforcement every day." He stated that "[w]e have a staff of professionals, including former law enforcement personnel, on call 24 hours a day, seven days per week to assist law enforcement with lawful requests…[and] [t]his work is significant." Neuenschwander claimed that "[o]ver the past 7 years, the company has responded to over 127,000 requests from U.S. law enforcement agencies for information that we've been told is critical to helping prevent or solve crimes." He stated that "[i]n addition, our teams have fielded and supported thousands of emergency requests from U.S. law enforcement, typically taking action within twenty minutes of receipt…[a]nd the number of U.S. government requests has increased over 100%, indicating that the information we are providing is valuable to investigations."

Neuenschwander stated that "[g]iven the pace of innovation and the growth of data in recent years, we understand that one of the biggest challenges facing law enforcement is a lack of clear information about what data are available, where they are stored, and how they can be obtained." He remarked that "[t]hat is why we publish a comp [w]rehensive law enforcement guide that

provides this information, and our team has trained law enforcement officers in the United States and around the world on these processes…[and]e will continue to increase our training offerings in the future, including by deploying online training to reach smaller law enforcement departments.

Facebook Product Management Director for Privacy and Integrity in Messenger Jay Sullivan claimed that "[i]mplementation of encryption does not undercut our commitment to cooperating with law enforcement." He asserted that "[l]aw enforcement will still receive valuable information in response to lawful requests." Sullivan stated that "[f]or example, encryption will have no effect on our responses to lawful requests in providing metadata, including potentially critical location or account information…[n]or will Facebook's end-to-end encryption interfere with law enforcement's ability to retrieve messages stored on a device." He stated that "[p]eople will also still be able to report concerning content to us, and we will be able to provide that content to law enforcement when appropriate…[a]nd we will continue to provide unencrypted content from the Facebook family of apps—including content from the public spaces of Instagram and Facebook, which we do not plan to encrypt—in response to lawful requests."

Sullivan stated that "[s]ome have called for "exceptional access"—the building of "backdoors" in otherwise secure systems…[and] [w]e oppose intentionally weakening the security of encrypted systems to create a "backdoor" because doing so would undermine the privacy and security of our users everywhere and would leave billions of people vulnerable to hackers or other unauthorized access." He argued that "[y]ou cannot build a backdoor for one person and not expect others to try to open it." Sullivan stated that "[w]hen people send messages with an encrypted service, they trust that those messages won't be seen by anyone else, including Facebook." He argued that "[w]eakening encryption to create a backdoor would erode that trust…[a]nd it would encourage people to move to encrypted services that do not have the same resources, expertise, and commitment to safety as Facebook." Sullivan pointed out that "[w]e can be certain that if we build a backdoor for the U.S. government, other governments, including repressive and authoritarian regimes around the world, will demand access or try to gain it clandestinely, including to persecute dissidents, journalists, and their political opponents." Sullivan claimed that "[p]reserving the prominence of American values online requires strong protections for privacy and security, including strong encryption."

Sullivan said that "[i]nstead of weakening encryption as a security technology, we are working with others to develop ways to use information we can access to support law enforcement when it is lawful and appropriate." He stated that "[w]e have made meaningful progress on cross-industry safety work in recent years, and it has been a group effort, through efforts like Microsoft's PhotoDNA used to identify child exploitation imagery, our partnership with the Tech Coalition and NCMEC on child safety, the Global Internet Forum to Counter Terrorism that helps coordinate the fight against terrorism online, and our partnerships with more than 100 global partners on our suicide prevention work." Sullivan claimed that "[m]ost recently, we open-sourced photo- and video-matching algorithms that can help smaller companies keep people safe on their online platforms…[and] [t]his is truly a cross-industry, private- and public-sector team effort, and Facebook has been a pioneer in developing and adopting tools and encouraging other industry participants to do the same for their platforms."

Oversight Hearing On Federal Cybersecurity

The House Oversight and Reform Committee's Government Operations Subcommittee held its most recent oversight hearing into the implementation of the "Federal Information Technology Acquisition

Reform Act" (FITARA) (P.L. 113-291). The Subcommittee released its ninth FITARA Scorecard that showed improvement for federal agencies in how they are securing their information systems. However, like all the other Scorecards, this one shows room for improvement, and the Government Accountability Office (GAO) pointed to a number of unfilled recommendations as much of the reason for the lacking cybersecurity.

Chair Gerry Connolly (D-VA) stated that "[s]ince the enactment of the Federal Information Technology Acquisition Reform Act (FITARA) in 2014, this Subcommittee has maintained steady and bipartisan oversight of agency implementation of the law." He claimed that "[t]he benefits of this continued oversight are clear: across the government, agencies have improved federal information technology (IT) acquisition." Connolly stated that "[i]n fact, the FITARA Scorecard's success has led this Subcommittee to incorporate other aspects of federal IT into the grades." He asserted that "[t]his Subcommittee has augmented and changed the scorecard to take cognizance of other important components of federal IT, such as cybersecurity, and incorporated other constructive feedback from agencies." Connolly contended that "[t]oday, the scorecard incorporates grades adapted from three additional pieces of legislation, including the MEGABYTE Act, the Modernizing Government Technology (MGT) Act, and the Federal Information Security Management Act (FISMA)…[but] [t]he bottom line is that the FITARA scorecard works and continues to hold agencies accountable for implementing the best IT practices."

Connolly stated that "[i]n November 2015, the average FITARA grade was a 'D' across all participating agencies…[and] [o]ver the past four years, agencies have incorporated new, sometimes challenging metrics and higher stakes, and yet, the average overall agency grade today is trending up — now above a 'C.'" He stated that "[u]nfortunately for some agencies, and in some categories, progress has slowed…[and] I hope to hear from our witnesses and GAO about what it takes to move beyond these hurdles to ensure efficient IT acquisition and management practices." Connolly stated that "[w]e must continue to see the dividends from putting resources towards modernizing legacy IT systems, migrating to the cloud, and maintaining a strong cyber posture."

Connolly stated that "[a]t our last hearing, the Federal CIO, Suzette Kent, testified that she would continue the push for aggressive data center closures in the Office of Management and Budget's revised Data Center Optimization Initiative (DCOI) policy." He contended that "[i]n June, OMB released new agency data center guidance that changed the entire baseline for how agencies define and count data centers." Connolly stated that "[j]ust one year ago, agencies reported on more than 4,700 data centers that they planned to continue to operate…[and] [i]n the 2019 data center inventory, however, this number dropped by nearly 50% to 2,400 data centers." He stated that "we don't think this demonstrates progress…[and] OMB appears to have made a definitional change without justification — and perhaps, an accounting trick." He stated that "I also question whether OMB's narrow definition of a data center leaves out facilities that the government should still be tracking even if these data centers are not candidates for consolidation or closures." Connolly stated that "[d]ata centers remain a cybersecurity vulnerability, and we cannot simply write off the risk because OMB decided to change the standard to artificially show progress."

Ranking Member Mark Meadows (R-NC) said that efficient procurement and use of IT has broad support from both parties despite not being a high-profile issue. He said the Subcommittee pays very close attention to the issue and has indirectly become part of the appropriations process. Meadows said the Subcommittee wants to make it part of the appropriations process in a formal sense where agencies are rewarding for effective FITARA implementation. He declared that efficiency in government as it relates to IT is critical, and he added "we spend more on IT than we

should." Meadows asserted the federal government is spending more than $100 billion a year and needs to do a better job. He said he is committed on both the "fiscal side of things" and the "reform side of things" to work with all the agencies on federal IT.

Government Accountability Office (GAO) Information Technology Acquisition Management Issues Director Carol Harris stated that "[f]ederal agencies and the Office of Management and Budget (OMB) have taken steps to improve the management of information technology (IT) acquisitions and operations and ensure the nation's cybersecurity through a series of initiatives." She stated that "[a]s of November 2019, federal agencies had fully implemented 61 percent of the 1,320 IT management-related recommendations that GAO has made to them since fiscal year 2010…[and] [l]ikewise, agencies had implemented 76 percent of the 3,323 security-related recommendations that GAO has made since fiscal year 2010."

Harris stated that "[s]ignificant actions remain to be completed to build on this progress:

- **Chief Information Officer (CIO) responsibilities**. Laws such as the Federal Information Technology Acquisition Reform Act (FITARA) and related guidance assign 35 key responsibilities to agency CIOs to help address longstanding IT management challenges. In August 2018, GAO reported that none of the 24 selected agencies had established policies that fully addressed the role of their CIO. GAO recommended that OMB and the 24 agencies take actions to improve the effectiveness of CIOs' implementation of their responsibilities. Although most agencies agreed or did not comment, none of the 27 recommendations have yet been implemented.
- **CIO IT acquisition review**. According to FITARA, covered agencies' CIOs are required to review and approve IT contracts. Nevertheless, in January 2018, GAO reported that most of the CIOs at 22 covered agencies were not adequately involved in reviewing billions of dollars of IT acquisitions. Consequently, GAO made 39 recommendations to improve CIO oversight for these acquisitions. Since then, 23 of the recommendations have been implemented.
- **Consolidating data centers**. OMB launched an initiative in 2010 to reduce data centers. In August 2018, 22 agencies reported that they had achieved $1.94 billion in cost savings for fiscal years 2016 through 2018, while two agencies reported that they had not achieved any savings. GAO has made 196 recommendations to OMB and agencies to improve the reporting of related cost savings and to achieve optimization targets. As of November 2019, 121 of the recommendations have been implemented.
- **Managing software licenses**. Effective management of software licenses can help avoid purchasing too many licenses that result in unused software. In May 2014, GAO reported that better management of licenses was needed to achieve savings, and made 135 recommendations to improve such management. As of November 2019, all but 19 of the recommendations had been implemented.
- **Ensuring the nation's cybersecurity**. While the government has acted to protect federal information systems, GAO has consistently identified shortcomings in the federal government's approach to cybersecurity. The 3,323 recommendations that GAO made to agencies since 2010 have been aimed at addressing cybersecurity challenges. These recommendations have identified actions for agencies to take to fully implement aspects of their information security programs and strengthen technical security controls over their computer networks and systems. As of November 2019, 76 percent of the recommendations had been implemented."

Assistant Director Leaving CISA

The Department of Homeland Security (DHS) named Assistant Secretary of Homeland Security for Cyber, Infrastructure, and Resilience Policy Bryan Ware as the replacement for Assistant Director for Cybersecurity for the Cybersecurity and Infrastructure Security Agency (CISA) Jeanette Manfra who announced her intention to step down before the end of calendar year 2019. This position does not require Senate confirmation, but the White House will need to sign off on the nomination before Ware can replace Manfra. Ware would inherit Manfra's wide-ranging portfolio, including the election security and supply chain efforts she helmed at CISA, and would face Congress on future occasions as Manfra has testified numerous times over the last few years.

According to his DHS biography:

> Mr. Ware is an entrepreneur, founding an artificial intelligence company in 1998 which he led as CEO through multiple rounds of Venture Capital investment until it was acquired in 2013 by Haystax. After serving as CTO of Haystax for several years during which he helped the company acquire leading cloud technology and cybersecurity companies, Bryan took over as CEO of Haystax in 2016 until its acquisition in 2018. Mr. Ware started his professional career at leading Defense contractors working on advanced technology programs like the Star Wars program, early UAV payloads, and counterterrorism technologies. Mr. Ware has been issued multiple patents in artificial intelligence and mobile technology. He holds a degree in Applied Optics from Rose-Hulman Institute of Technology.

Before serving as the first Assistant Director for Cybersecurity at CISA, Manfra was the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) for the former National Protection and Programs Directorate (NPPD), CISA's forerunner. Manfra will go to work for Google Cloud just after the start of the new year. Incidentally, Google Cloud announced that FedRAMP had bestowed a high authorization to operate "for 17 products in five cloud regions."

Facebook Issues Opinion and Final Order Against Cambridge Analytica

The Federal Trade Commission (FTC) issued an opinion and a final order against Cambridge Analytica for its actions in using the data of up to 87 million Facebook users in the 2016 election. The FTC found that Cambridge Analytica violated Section 5 of the Federal Trade Commission Act (FTC Act) by engaging in unfair and deceptive practices. The FTC also found that Cambridge Analytica violated the European Union-United States Privacy Shield by claiming to adhere to the trans-Atlantic data flow agreement even though its certification had lapsed. Moreover, the agency claimed the company violated the agreement as well.

However, Cambridge Analytica has filed for bankruptcy and did not respond to the FTC's allegations, giving the agency free rein in making its allegations and meting out punishment. In the opinion, FTC Commissioner Noah Joshua Phillips noted that the agency made "a determination that Cambridge Analytica made false or misleading representations in violation of Section 5 of the FTC Act:

- to Facebook users who authorized the GSRApp that it did not collect their personally identifiable information (Count I);
- that it was a participant in Privacy Shield from May to November 2018, even though it had allowed its certification to lapse (Count II); and

- that it would adhere to Privacy Shield principles, even though it failed to affirm to the Department of Commerce, as required, that it would continue to apply those principles to personal information it had acquired while participating in the program (Count III).

Phillips explained the salient points of the final order:

- Paragraph I of the Final Order prohibits Respondent from making misrepresentations regarding the extent to which it protects the privacy and confidentiality of Covered Information as defined in the Final Order, including: (1) the extent to which it collects, uses, shares, or sells any Covered Information; and (2) the purposes for which it collects, uses, shares, or sells any Covered Information.
- Paragraph II prohibits Respondent from making misrepresentations, in connection with any product or service, regarding the extent to which Respondent participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including, but not limited to, the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.
- Paragraph III imposes additional requirements to address Respondent's unlawful conduct related to its participation in and compliance with the Privacy Shield framework. Specifically, Paragraph III prohibits Respondent from possessing or controlling personal information from European Union residents that Respondent received while it participated in the EU-U.S. Privacy Shield framework unless Respondent complies with the requirements of either Paragraph III.A or Paragraph III.B. Paragraph III.A requires Respondent to affirm to Commerce within specified time limits that it: (1) will continue to apply Privacy Shield protections to the personal information it received while it participated in the Privacy Shield; or (2) will protect such information by another means authorized under EU or Swiss law. Alternatively, Paragraph III.B requires Respondent to return or delete such personal information within specified time periods.
- Paragraph IV of the Final Order relates to the deletion or destruction of Covered Information collected from consumers through the GSR App, and any information or work product, including any algorithms or equations, derived in whole or in part from such Covered Information. Paragraph V permanently enjoins Respondent from disclosing, using, selling, or receiving any benefit from any Covered Information or any information that derived in whole or in part from it. Paragraph VI imposes access and monitoring requirements, and Paragraph VII provides that the Final Order will remain in effect for twenty years.

In July, the. FTC formally announced its long awaited $5 billion settlement with Facebook arising from its partnership with Cambridge Analytica in violation of a 2012 settlement. However, the FTC was not unanimous. In approving the settlement, the FTC split along partisan lines 3-2 with the two Democratic Commissioners voting against the settlement. In November 2011, the FTC and Facebook agreed on a draft consent order regarding the agency's allegations that Facebook violated Section 5 of the FTC Act through its privacy practices, and the FTC issued a final order in August 2012.

In a blog posting, the FTC explained the new requirements Facebook must meet:

- Facebook must implement a stringent program to monitor third-party developers and terminate access to any developer that doesn't follow the rules.
- In addition, Facebook can't use for advertising purposes the phone numbers it obtained specifically for security.

- When it comes to facial recognition technology, the order requires Facebook to give clear notice of how it uses that information and it must get consumers' express consent before putting that data to a materially different use.
- Facebook also will have to encrypt passwords and can't ask people for their passwords to other services, and must report any privacy incident to the FTC within 30 days.
- On top of everything Facebook will have to do to protect consumers' privacy, it also has to implement a comprehensive data security program.
- Another important consideration: These new accountability provisions don't just apply to Facebook. They also apply to companies Facebook controls, like Instagram, WhatsApp, and other Facebook-owned affiliates that it shares consumers' information with between now and 2039.

Bill Introduced To Give CISA Authority To Issue Subpoenas

The Senate Homeland Security Committee has released a long-anticipated bill that would provide the Cybersecurity and Infrastructure Security Agency (CISA) the authority to serve subpoenas on internet service providers (ISPs) to turn over the contact information of the owners of critical infrastructure with vulnerabilities. Chairman Ron Johnson (R-WI) and Senator Maggie Hassan (D-NH) are cosponsoring the "Cybersecurity Vulnerability Identification and Notification Act of 2019," a bill that was introduced in response to a legislative proposal submitted by the Department of Homeland Security (DHS) this summer.

In requesting subpoena authority, DHS allegedly had the operators of industrial systems in mind. Notably, administrative subpoenas can be issued by a number of law enforcement agencies without assent from a court. DHS officials have claimed the power would be used sparingly and only to make the owners and operators of some at risk critical infrastructure "more motivated." At present, ISPs cannot turn over the identity of its customers to a government agency absent a subpoena or a warrant, and law enforcement agencies can typically only issue administrative subpoenas as part of an investigation. Consequently, CISA, which lacks this authority, can seek and obtain the ownership of critical infrastructure that is at risk by piggybacking on a sister agency's authority. CISA is asking for its own standalone authority to clear up these problems.

Earlier this year, CISA's soon to depart Assistant Director for Cybersecurity and Communications Jeannette Manfra told reporters '[a] challenge that we have is that we can see a lot of industrial control systems...that have potential vulnerabilities that are accessible from the public internet." Supposedly, CISA can only ask the ISP to pass along its concerns or intelligence to targeted owners or operators. Speaking publicly also this past summer, CISA Director Christopher Krebs remarked that "[w]hat we want to be able to do is if we can't resolve the issue through any other way, then we should be able to go to an ISP and say, 'We're concerned about this, can you provide us your customer contact information so we can go let them know that they have whatever port open or are running a vulnerable system." When asked if DHS might not read and use its authority as expansively as possible as many agencies do, Manfra claimed "[w]e have a long history of collecting similar types of data through voluntary programs and [have] demonstrated ways of protecting that, as well as to ensure that the information is only used for the purposes that it was collected." She contended that CISA would use this authority in "very narrow set of circumstances."

The "Cybersecurity Vulnerability Identification and Notification Act of 2019" would expand the authority of CISA's National Cybersecurity and Communications Integration Center (NCCIC) to include "detecting, identifying, and receiving information about security vulnerabilities relating to

critical infrastructure in the information systems and devices of Federal and non-Federal entities for a cybersecurity purpose" and in order to fulfill these responsibilities, the agency would be able to issue subpoenas to ISPs. Specifically, "[i]f the Director identifies a system connected to the internet with a specific security vulnerability and has reason to believe that the security vulnerability relates to critical infrastructure and affects an enterprise device or system owned or operated by a Federal or non-Federal entity, and the Director is unable to identify the entity at risk, the Director may issue a subpoena for the production of information necessary to identify and notify the entity at risk, in order to carry out" the agency's new responsibilities to detect, identify, and receive information relating to threats to critical infrastructure. In response to a subpoena, the only information the ISP need turn over to CISA is name; address; length of service (including start date) and types of service utilized; and telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address. CISA then has 7 days to notify the at-risk entity.

The scope of the type of systems for which CISA may issue subpoenas is limited to an "enterprise device or system," which rules out consumer devices and systems. The term is defined as

- a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and
- does not include personal devices and systems, such as consumer mobile devices, home computers, residential wireless routers, or residential Internet enabled consumer devices.

There would be limits on CISA's use of the information obtained by subpoena, and the agency may only use information for a "cybersecurity purpose" (i.e. "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.") Additionally, CISA must immediately destroy any irrelevant information turned up by the subpoena and must do the same with any personally identifiable information unless the subject of the subpoena agrees otherwise.

Moreover, ISPs would receive liability protection for turning over this information in response to a CISA subpoena. If any duly served entity fails to comply with a subpoena, CISA may ask the Department of Justice to seek to enforce the subpoena in federal court.

In their press release, Johnson and Hassan stated "[i]n June 2019, DHS submitted a legislative proposal to Congress that would authorize the CISA to issue administrative subpoenas to telecommunications companies in an effort to identify owners and operators of critical infrastructure systems and devices that were at risk to cyberattacks." The claimed the bill would do the following:

- The legislation gives CISA a limited authority to detect, identify, and receive information only related to critical infrastructure systems for a cybersecurity purpose.
- The purpose of this legislation is to provide CISA the legal means necessary to notify the owner of the critical infrastructure system who was the subject of the subpoena, as a result CISA must notify the vulnerable party within 7 days of receiving their information. Additionally, to ensure the privacy of affected parties or entities CISA must destroy personally identifiable information (PII) after 6 months.
- The legislation includes an annual report to both Congress and the public. It requires reporting on the number of cybersecurity vulnerabilities that have been mitigated and number of entities warned because of this new authority. This allows Congress and the public to better understand whether CISA's administrative subpoena program has been effective at making U.S. critical infrastructure more secure.

- The bill requires subpoenas to be authenticated by electronic signature, or similar future technology, so that the internet service provider (ISP) knows it is coming from CISA and has not been fraudulently generated to unlawfully access the PII of ISP subscribers.

NIAC Calls For Major Reorganization of Federal Cyber Efforts

An advisory group to the President has recommended radical steps to change the cyber posture of the United States, including the creation of a new, independent cyber agency, the establishment of another executive branch agency to coordinate information sharing, the use of existing legal authority to require the owners and operators of critical infrastructure to implement "cyber mitigations," and legal protection for entities to blacklist and whitelist cyber products. Some of these steps could be taken with existing legal authority while others would require acts of Congress. These recommendations are made in the context of the ongoing cyber operations of nation states like Russia and China and groups not formally affiliated with any government.

The President's National Infrastructure Advisory Council (NIAC) is one of the advisory bodies housed within the Department of Homeland Security to advise the President on cybersecurity. In September, the National Security Council tasked President's National Infrastructure Advisory Council (NIAC) with examining "how the federal government and private industry can collaborate seamlessly to confront urgent cyber risks in the most critical and highly targeted private infrastructure." NIAC has returned what it considers pressing findings that require immediate and dramatic action. NIAC explained that "escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security…[and] U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win against nation-states intent on disrupting or destroying our critical infrastructure." NIAC claimed that "[b]old action is needed to prevent the dire consequences of a catastrophic cyber-attack on energy, communication, and financial infrastructures."

In terms of the boldest recommendations, NIAC calls for the President to create a new federal agency, the Federal Cybersecurity Commission (FCSC) by executive order, and a new entity, the Critical Infrastructure Command Center (CICC). The FCSC would be "an independent U.S. government entity to mitigate catastrophic cyber risks to critical infrastructure that have potential national security impacts….for the streamlining of regulatory authorities to achieve cyber mitigations in the private sector and counter extraordinary cyber threats, in consultation with an executive partnership of industry executives and government leaders." And yet, the "FCSC would not replace existing regulatory and oversight agencies…would serve as a bridge between the government and the identified companies in the energy, financial services, and communications sectors to help mitigate the most urgent cyber issues." The CICC would be established "to improve the real-time sharing and processing of private and public data—including classified information—between co-located government intelligence analysts, cyber experts from companies at greatest risk…and key government agencies, including sector-specific agencies, law enforcement, and the intelligence community."

Moreover, NIAC suggests that President utilize existing legal authorities "to direct the private sector to implement cyber mitigations" and then ask Congress for any additional legal authority to ensure the private sector must implement "cyber mitigations." Regarding the recommendation to modernize legal authorities, NIAC stated that "[a]n initial analysis conducted by the Working Group indicates that the Defense Production Act, the Federal Power Act, and the SAFETY Act all contain provisions that could enable the government to direct cyber mitigations in critical infrastructure sectors and

provide liability protections to companies that implement certain technologies." However, NIAC claimed that "more guidance and interpretation from the federal government is needed to understand the extent of these powers and under what circumstances they could be used in response to nation-state cyber threats."

NIAC added that "[t]he nation is not sufficiently organized to counter the aggressive tactics used by our adversaries to infiltrate, map, deny, disrupt, and destroy sensitive cyber systems in the private sector…[and] [t]o fix this, the Council recommends the following actions:

Make Cyber Intelligence Actionable

1. Establish the Critical Infrastructure Command Center (CICC) to improve the real-time sharing and processing of private and public data—including classified information—between co-located government intelligence analysts and cyber experts from companies at greatest risk (Section 9(a), E.O. 13800). The CICC will foster the trust and collaboration essential to develop the actionable intelligence and threat mitigations needed to counter rapidly evolving threats to our nation's critical infrastructure.
2. Direct the Intelligence Community to raise the priority of collecting, detecting, identifying, and disseminating information on efforts by nation-state and non-state actors to exploit, deny, or otherwise attack critical infrastructure in the United States. This should be a Priority 1 topic within the National Intelligence Priorities Framework.
3. Conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to CEOs of identified energy, communications, and financial services companies to build a compelling case for company action to counter serious cyber threats and to facilitate operationalizing the CICC.
4. Use the upcoming National Level Exercise 2020 to pilot the CICC model by bringing together cleared private sector experts with intelligence officers and representatives from other key government agencies, such as law enforcement and sector-specific agencies, to collaboratively analyze classified threats and understand resulting consequences to critical infrastructure.

Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission

5. Issue an Executive Order to create the Federal Cybersecurity Commission (FCSC) as an independent U.S. government entity to mitigate catastrophic cyber risks to critical infrastructure that have potential national security impacts. The Commission offers a bold new approach for the streamlining of regulatory authorities to achieve cyber mitigations in the private sector and counter extraordinary cyber threats, in consultation with an executive partnership of industry executives and government leaders.
6. Convene a symposium of select Cabinet Secretaries, regulators, Office of Management and Budget (OMB) officials, CEOs, and industry representatives to clarify the functions, roles, responsibilities, and processes of the Commission, based on the more detailed work done by the NIAC.

Modernize Legal Authorities to Improve Cyber Defense

7. Direct the Department of Justice to analyze existing legal authorities to determine the ability of government to direct the private sector to implement cyber mitigations and to identify legal barriers that prevent the private sector from implementing

requested mitigations and sharing information with the government, based on the more detailed work done by the NIAC.

Secure the Supply Chain of Critical Cyber Components

8. Provide liability protection to allow blacklisting and whitelisting of critical cyber products used in private critical infrastructure, similar to the authority provided in 10 CFR Part 21 for the nuclear industry and to the Department of Energy's (DOE) enhanced procurement authority.

9. Continue and expand programs at the DOE's national laboratories and other ongoing initiatives to independently test vendor equipment for vulnerabilities and report the results to private companies.

NIAC claimed that "America's companies are fighting a cyber war against multi-billion-dollar nation-state cyber forces that they cannot win on their own…[and] [i]ncremental steps are no longer sufficient; bold approaches must be taken."

EDPB Explains Extra-Territorial Scope of GDPR

The European Data Protection Board (EDPB or Board), an entity consisting of the European Union's (EU) data protection authorities, has released guidance regarding the territorial scope of the General Data Protection Regulation (GDPR). This guidance represents "a common interpretation by data protection authorities in the EU," and therefore will "ensure a consistent application of the GDPR when assessing whether particular processing by a controller or a processor falls within the scope of the new EU legal framework." Moreover, "[a]s a general principle, the EDPB asserts that where the processing of personal data falls within the territorial scope of the GDPR, all provisions of the Regulation apply to such processing." Consequently, any entities that collect and process the personal data of EU citizens will need to analyze whether they may fall into the GDPR despite not having a physical presence on the continent.

The EDPB "underlines that the application of Article 3 aims at determining whether a particular processing activity, rather than a person (legal or natural), falls within the scope of the GDPR." The Board added "[c]onsequently, certain processing of personal data by a controller or processor might fall within the scope of the Regulation, while other processing of personal data by that same controller or processor might not, depending on the processing activity."

Article 3 of the GDPR stipulates that it applies:

- to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
- to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    - the monitoring of their behaviour as far as their behaviour takes place within the Union.
- to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

The EDPB asserted that "Article 3 of the GDPR reflects the legislator's intention to ensure

comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows."

The EDPB explained that when either the "establishment" criterion or the "targeting" criterion are met, then a data controller or processor, regardless of its physical location, will be subject to the GDPR's requirements. Additionally, where a public international law allows an EU's laws to control processing or data, then the GDPR will also attach to these activities, but the exmaples presented in the guidance pertain mostly to the processing of data outside of the EU by entities that are clearly subject to the EU's jurisdiction.

The Board explained "Article 3(1) ensures that the GDPR applies to the processing by a controller or processor carried out in the context of the activities of an establishment of that controller or processor in the Union, regardless of the actual place of the processing." The EDPB "therefore recommends a threefold approach in determining whether or not the processing of personal data falls within the scope of the GDPR pursuant to Article 3(1):

- first by considering the definition of an 'establishment' in the EU within the meaning of EU data protection law,
- second by looking at what is meant by 'processing in the context of the activities of an establishment in the Union', and
- lastly by confirming that the GDPR will apply regardless of whether the processing carried out in the context of the activities of this establishment takes place in the Union or not.

In order for the GDPR to attach to a non-EU entity, it must be established in the EU. The EDPB explains that having as few as one employee stationed in the EU could make a non-EU entity subject to the GDPR but this employee must have a connection to the data processing activities of the entity. But, the Board admits there are limits to this doctrine, notably that "[i]t is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking's website is accessible in the Union."

Once it has been proved that an entity is established in the EU, "[i]f a controller or processor established outside the Union exercises "a real and effective activity - even a minimal one" - through "stable arrangements", regardless of its legal form (e.g. subsidiary, branch, office...), in the territory of a Member State, this controller or processor can be considered to have an establishment in that Member State."

Regarding the "targeting" provisions of Article, the EDPB stated that "[t]he absence of an establishment in the Union does not necessarily mean that processing activities by a data controller or processor established in a third country will be excluded from the scope of the GDPR, since Article 3(2) sets out the circumstances in which the GDPR applies to a controller or processor not established in the Union, depending on their processing activities." The EDPB stated that "[w]hile the present guidelines aim to clarify the territorial scope of the GDPR, the EDPB also wish to stress that controllers and processors will also need to take into account other applicable texts, such as for instance EU or Member States' sectorial legislation and national laws.

The EDPB added that

> The application of the "targeting criterion" towards data subjects who are in the Union, as per Article 3(2), can be triggered by processing activities carried out by a controller or

processor not established in the Union which relate to two distinct and alternative types of activities provided that these processing activities relate to data subjects that are in the Union. In addition to being applicable only to processing by a controller or processor not established in the Union, the targeting criterion largely focuses on what the "processing activities" are "related to", which is to be considered on a case-by- case basis.

The EDPB stressed "that a controller or processor may be subject to the GDPR in relation to some of its processing activities but not subject to the GDPR in relation to other processing activities...[and] [t]he determining element to the territorial application of the GDPR as per Article 3(2) lies in the consideration of the processing activities in question." The EDPB recommended "a twofold approach, in order to determine first that the processing relates to personal data of data subjects who are in the Union, and second whether processing relates to the offering of goods or services or to the monitoring of data subjects' behaviour in the Union."

Further Reading

- "Made in America: White House veterans helped Gulf monarchy build secret surveillance unit" – *Reuters*. The latest in the saga Reuters has been telling as former top intelligence officials like Richard Clarke helped the United Arab Emirates build a surveillance program using National Security Agency know-how that was initially focused on the security of UAE but over time grew to include enemies of the state outside the country, including the United Nations and Americans. The organizations that set up and largely ran this program may have been operating in a gray area of U.S. law regarding the use of national security skills obtained in the employ of the U.S. government. Some former officials are calling for tighter regulation of when and how former U.S. Intelligence Community personnel can work for other nations.
- "The Gospel of Wealth According to Marc Benioff" – *WIRED*. Benioff's charitable efforts may be strategic and ultimately all billionaire charity may not bridge the gap between those thriving in the West and those not thriving.
- "We Just Got a Rare Look at National Security Surveillance. It Was Ugly." – *The New York Times*. The Department of Justice's Office of the Inspector General released its investigation into the FISA process used to surveil members of the Trump campaign in 2016 and found major shortcomings in the process for FISA warrants and surveillance. This report could contribute to the bipartisan call for FISA reform.
- "Amazon Accuses Trump of 'Improper Pressure' on JEDI Contract" – *The New York Times*. Amazon is making President Donald Trump's voluminous comments about the company part of its protest against the Department of Defense's award of a $10 billion cloud computing contract to Microsoft and its subcontractors. Amazon is claiming that Trump's animus towards the company and its CEO Jeff Bezos sent the message to the Pentagon not to give the contract to the company even though it was considered the front-runner.
- "Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network" – *Gizmodo*. Amazon's Ring is becoming a de facto CCTV system in many urban and suburban areas, but policymakers and the public may not have thought through all the implications.
- "U.S. Justice Department to review Google's deal for Fitbit: source" – *Reuters*. Google's $2.1 billion deal to buy Fitbit is getting antitrust scrutiny at the Department of Justice. This investigation and other investigations into big tech may signal a sea change in how Washington will view future mergers.
- "She was Instacart's biggest cheerleader. Now she's leading a worker revolt." – *The Washington Post*. Like a number of other tech startups, Instacart is adjusting worker pay in

ways that will probably lead to more revenue but lower pay for the contractors who deliver orders. Some workers are organizing to fight back.

- "Cops see an encryption problem. Spyware makers see an opportunity." – *MIT Technology Review*. There are a number of vendors and methods available to law enforcement to get around encryption.