Technology Policy Update
23 January 2020
By Michael Kans, Esq.

House Judiciary Continues Tech Antitrust Hearings

House Judiciary Committee's Antitrust, Commercial, and Administrative Law Subcommittee continued its series of hearings titled "Online Platforms and Market Power" with a field hearing in Colorado titled "Competitors in the Digital Economy" that heard from small and mid-sized companies that have encountered difficulties working with and competing against large platforms. These firms claimed that companies like Amazon and Google abused their market power to extract greater concessions from these companies.

Subcommittee Chair David Cicilline (D-RI) stated that "[i]n July, the Subcommittee received testimony from executives representing the four dominant online platforms—Google, Amazon, Facebook, and Apple—along with a panel of leading experts about the effect of market power in the digital economy on innovation and entrepreneurship." He contended that "[t]hrough both that hearing and other parts of the Subcommittee's investigation, it has become clear that these firms have tremendous power as gatekeepers to shape and control commerce online." Cicilline said that "[a]s Stacy Mitchell, the Director of the Institute for Local Self Reliance, testified:

> A growing share of our commerce now flows through a handful of digital platforms. These powerful gatekeepers not only control market access, but also directly compete with the businesses that depend on them.

Cicilline stated that "[i]t is apparent that the dominant platforms are increasingly using their gatekeeper power in abusive and coercive ways….[and] [b]ecause these platforms function as bottlenecks for online commerce, they are able to set the terms and conditions of competition, giving them immense power to pick winners and losers in the online economy." He asserted that "[i]t is far too common to hear horror stories from startups and other small businesses about how a dominant platform's abrupt changes have destroyed their business." Cicilline said that "[a] single sudden change to an algorithm, a software update, or new product design can be disastrous for the millions of companies that depend on these platforms to get to market."

Cicilline stated that "[a]nd because these platforms actively compete with the very businesses that rely on them, what may be portrayed as an innocent change could very well be a deliberate strategy to crush any existing or potential competition." He contended that "[c]ompanies across the online ecosystem, both large and small, have found themselves dependent on the arbitrary whim of these platform giants, one algorithm tweak away from ruin." Cicilline argued that "[i]n many cases, there is little notice or any real recourse for the companies that are disadvantaged by the platforms' conduct…[and] [b]ecause their decisions are largely unaccountable, opaque, and result in sweeping consequences, the dominant platforms effectively serve as private regulators."

Cicilline claimed that "[t]he dominant platforms can also use their gatekeeper power to dictate anti-competitive, take-it-or-leave it contract terms." He noted that "[s]tartups and small businesses have had to sign away certain basic rights or hand over valuable data to a competitor as the price of

accessing their customers through the platform." Cicilline declared that "[s]uch coercive terms of doing business would undoubtedly be absent in a competitive marketplace."

Cicilline stated that "[f]or locally-owned businesses that are the economic lifeblood of their communities as both job creators and engines of prosperity, this gatekeeper power—and how the platforms are exercising it—is of tremendous concern…[and] [m]any small businesses are forced to rely on dominant platforms to advertise or sell their products and services online. In many cases, they do not have an alternative." Cicilline remarked that "[e]arlier this week, my staff spoke with an online seller whose entire economic livelihood and his family's health has been jeopardized by one of the dominant platform's sudden, arbitrary, and reckless decision to suspend his business and block access to his inventory." He stated that "[n]ot only does this dynamic threaten ongoing competition, but it also has lasting effects as a powerful disincentive for new entrants to try and compete with powerful incumbents."

Cicilline stated that "[a]s Patrick Spence, the CEO of Sonos, will testify today, this shuttering of competition online

> dries up the venture capital new companies need to develop the next great inventions and bring them to market. Venture capital firms are well aware of the kill zone that surrounds start ups that pass within striking distance of the dominant platforms—they stay away from those investments.

Cicilline said that "[t]oday, we will hear from the CEOs, founders, and senior executives of several dynamic and innovative companies that must confront this economic nightmare." He added that "[e]ach of the innovative companies represented here today—Sonos, PopSockets, Tile, and Basecamp—are American success stories…[and] I applaud them for their courage to share their testimony in the face of potential retaliation by the dominant platforms." Cicilline claimed that "[w]e have been in touch with a number of companies with similar perspectives that, understandably, will not testify due to this very real concern."

Representative Ken Buck (R-CO) claimed that as the subcommittee continues its oversight of state of competition in the tech sector, the focus is shifting from hearing how larger platforms operate to hearing how it is trying to compete with these platforms. He said that each of the panelists represent companies in the arena, innovating and competing daily to deliver value to customers. Buck declared "they have real skin in the game" and said he looks forward to hearing from their unique perspectives. He articulated the principles he believes Congress should be using in its inquiry:

> 1. Innovation and competition in the tech sector have produced enormous value for consumers. We should not forget about those benefits as we consider the current state of competition in the tech sector.
> 2. Any legislative proposals that emerge from our inquiry should be consistent with maintaining a free and competitive marketplace. For proposals to construct broad and new regulatory regimes must be viewed with caution. Experience has shown that burdensome regulations often miss the mark. Regulations often come too late to change anything and this approach is often less efficient than the free market. Regulators are often not nimble enough to keep pace with the dynamic marketplace so that the regulatory regime has the effect of entrenching incumbents rather than encouraging competition.

3. Big is not necessarily bad. Antitrust laws do not exist to punish success but to promote competition. Congress should help foster an atmosphere where ideas flourish and startups can innovate, fairly compete, grow, and succeed.

Buck said with these principles in mind, over the past few years, the largest platforms have continued to expand and increase their market power. He asserted that the increased competition and market power of a small group of companies has raised these concerns from a diverse array of constituencies about how that power is being used, including domestic and international regulators, enforcement authorities, small, medium and large companies and consumers. Buck asserted the subcommittee's task during the hearings has been to evaluate whether true antitrust harms are occurring in the tech sector, and, if so, whether the existing antitrust laws are adequate to address these harms. He said that in order to understand these questions, a diverse panel of market participants have been invited, and these companies compete directly with the large platforms that rely on the services of the large platforms, and in some cases, both compete with and rely on a large platform.

Buck said these companies that compete with and rely on the large platforms have become more and more common as Google, Facebook, Amazon, and Apple have continued to expand into broader and more diverse business lines. He claimed that it is common knowledge that many tech companies rely on the infrastructure services provided by large platform companies in order to serve customers while simultaneously having to directly compete with these platform companies. Buck laid out a hypothetical in which Company A competes with Google products but also relies on a different Google product to run its business, and another in which Company B relies on Amazon or Apple for its success and then Amazon or Apple launches a new product that competes directly with Company B. Buck argued that in these circumstances the question arises as to line between fierce and healthy competition and anticompetitive conduct. He asked whether the large platforms use their market power in one area to harm competitors in another business line. Buck said if this does occur, how is it discerned whether the allegedly harmful conduct was motivated solely by a desire to improve the product or whether there was anticompetitive motive.

Sonos CEO Patrick Spence stated that "[d]ominant platforms are able to develop copycat products by analyzing sales metrics on their platforms and combining them with rich data profiles of their customers…[and] [t]hese copycat products are then sold at cost or lower, with no intent to reap a profit." Spence also stated that "[t]hey also can use remarkably similar trade dress and marketing campaigns." He contended that "[o]ur recently filed patent infringement case against Google makes the point." He stated that "[i]n 2013-14, we gave access to our technology to Google as part of a partnership to provide Google's music service to our customers…[and] [t]hen, in 2015 Google started producing more and more products that copy our key functionalities and infringe on our foundational intellectual property."

Spence stated that "my experience as a tech executive suggests some important areas for your exploration:

- Do the rules around predatory pricing make sense in today's economy?
- How do we limit the power of dominant players to leverage their business insights to create copycat private label products?
- How do we protect smaller firms from retaliation by dominant players for the assertion of legal rights?

- Should there be stronger firewalls between different business segments of the dominant platform players?
- How can we encourage interoperability and greater access to dominant platforms, so that consumers, and businesses, can choose what's best for them?"

Basecamp LLC Co-Founder and CTO David Heinemeier Hansson offered the "following policy ideas:

- Take inspiration from the DOJ ruling that required Microsoft to offer consumers a choice of browser when installing Windows. Users of the Chrome browser, the Firefox browser, the Android operating system, and the iOS operating system should be given a clear, upfront choice of which search engine they want to use. Google should not be able to pay $10+ billion/year to Apple to cement their search monopoly.
- Ban Google from selling advertisement on trademarked keywords to direct competitors. Google is able to extract enormous sums from the marketplace when competitors engage in ad wars, buying ads on each other's trademarked terms. The only winner is Google.
- Deny Apple the ability to discriminate against app developers who choose to go to a competitive market for payment processing. Allow them to clearly tell their customers what they're doing and direct them accordingly.
- Bring down the exorbitant fees for payment processing in the app stores to match what would have been the case in a competitive market. Reduce the rates from 30% to, say, 3%. We would be thrilled to give customers the most convenient way to buy our products if the rates were competitive.
- Ban the practice of targeting ads based on personal information, unless each piece of personal information used in the ads was specifically obtained with the voluntary, optional, and informed consent that it be used for marketing purposes. As in in the pregnancy example, "Yes, I give permission to Facebook to sell the fact that I'm pregnant to companies that want to advertise to pregnant women"
- Require Facebook and Google to disclose to people the complete dossier that's being used to target ads against them, and give people the option to flush that dossier.

House Oversight Facial Recognition Hearing

The House Oversight and Reform Committee held its third hearing on facial recognition technology and its first with new Chair Carolyn Maloney (D-NY). There continues to be consensus that public sector use of this technology should be sharply curtailed if not banned outright. However, there is not agreement on private sector use of facial recognition technology. It is too early to determine whether this gap between Republicans and Democrats may sink legislation Members on both sides of the dais claim they want enacted.

In her opening statement, Maloney remarked the committee "is holding our third hearing this Congress on a critical issue: facial recognition technology…[and] [i]t is clear that, despite the private sector's expanded use of the technology, it is just not ready for prime time." She said that "[d]uring this hearing, we will examine the private sector's development, use, and sale of the technology, as well as its partnerships with government entities using this technology." Maloney said that "[w]e learned from our first hearing on May 22 of 2019 that the use of facial recognition technology can severely impact Americans' civil rights and liberties, including the right to privacy, free speech, and equal protection under the law." She added that "[w]e learned during our second hearing on June 4 how federal, state, and local government entities use this technology on a wide scale, yet provide very little transparency on how and why it is being used—or on security measures to protect

sensitive data." She declared that "[d]espite these concerns, we see facial recognition technology being used more and more in our everyday lives."

Maloney stated that "[t]he technology is being used in schools, grocery stores, airports, malls, theme parks, stadiums, and on our phones, social media platforms, doorbell camera footage, and even in hiring decisions." She noted that "[t]his technology is completely unregulated at the federal level, resulting in some questionable and even dangerous applications." Maloney observed that "[i]n December 2019, the National Institute of Standards and Technology, or NIST, issued a new report finding that commercial facial recognition algorithms misidentified racial minorities, women, children, and elderly individuals at substantially higher rates."

Maloney stressed that "[o]ur examination of facial recognition technology is a bipartisan effort…[and] I applaud Ranking Member [Jim] Jordan's (R-OH) tireless and ongoing advocacy on this issue." She asserted that "[w]e have a responsibility to not only encourage innovation, but to protect the privacy and safety of American consumers…[and] [t]hat means educating our fellow Members and the American people on the different uses of the technology and distinguishing between local, subjective, identification, and surveillance uses." Maloney stated that "[t]hat also means exploring what protections are currently in place to protect civil rights, consumer privacy, and data security and prevent misidentifications, as well as providing recommendations for future legislation and regulation." She announced that "our Committee is committed to introducing and marking-up common-sense facial recognition legislation in the near future…[a]nd our hope is that we can do that on a truly bipartisan basis."

Ranking Member Jim Jordan (R-OH) stated his appreciation for Maloney's willingness to work with Republicans on legislation and said they have a bill, too. He contended that facial recognition technology is a powerful new tool that is widely being used by both government agencies and private sector companies. Jordan remarked that its sales have experienced a 20% year-to-year growth since 2016, and the market is expected to be valued at $8.9 billion by 2022. He contended that increasingly local and state governments are increasingly using this technology under the guise of law enforcement and public welfare but with little to no accountability. He asserted that with this technology, the government can capture faces in public places and identify individuals that allows the tracking of a person's movements, patterns, and behavior. Jordan noted all of this is currently happening without legislation to balance legitimate government functions with American civil liberties. He declared this must change.

Jordan remarked that while the hearing is about commercial uses of facial recognition technology, he stressed he has no intention of hampering technological advancement in the private sector. He said he understands the promise this technology holds in making everyone's life better. Jordan claimed it has already improved data security and made identity verification more efficient with respect to preventing theft and protecting consumers. He argued the urgent issue is reining in the government's unchecked use of this technology when it impairs freedoms and liberties. Jordan said that the late, former Chair Elijah Cummings (D-MD) became concerned about the government's use of facial recognition technology after learning it was used to surveil protests in his district after the death of Freddie Gray. He claimed Cummings saw this as a deeply troubling encroachment on the freedoms of speech and association, and Jordan said he could not agree more.

Jordan asserted that the issue transcends politics as the idea of Americans being tracked and catalogued for merely showing their face in public is deeply troubling. He said it is imperative that

Congress understands the effects of this technology on Constitutional liberties. Jordan asserted that the invasiveness of facial recognition technology has already led a number of localities to ban a number of government agencies from buying or using digital facial recognition for any purpose. He warned that this trend threatens to create a patchwork of laws and uncertainty and may impede legitimate uses of the technology. Jordan claimed this is an issue best not left to the courts.

Jordan asserted that facial recognition presents novel questions that are best answered by Congressional policymaking that can establish a national consensus. Jordan stated that a number of federal agencies possess facial recognition technology and use it without guidance from Congress despites its serious implications on First and Fourth Amendment rights and added that at the bare minimum, Congress must understand when and how agencies are using this technology and for what purpose. He asserted Congress does not possess this basic information. Jordan noted the unique jurisdiction of the committee over emerging technology across the federal government puts it in a position to consider policy solutions. He said that Republicans intend to introduce legislation that would provide transparency and accountability for the federal government's purchase and use of this technology and ideally in concert with Democrats.

Future of Privacy Forum Senior Counsel and Director of AI and Ethics Brenda Leong stated that "[s]hould Congress pursue facial recognition-specific legislation, there are several key points which should provide the foundation, as described in our Privacy Principles." She said that "[w]hile not sufficient to address all concerns, consent remains the critical factor, and should be tiered based on the level of personal identification collected or linked, and the associated increasing risk levels:

- No unique biometric identifier should be created and maintained over time without appropriate consent.
- For commercial applications using verification or identification systems, the requirement should bean "opt-in" model, that is, a default of express, affirmative consent consistent with existing FTC definitions, accepted practices, and expectations. Exceptions to this express consent requirement should be limited and narrow.
    - Use cases involving unique persistent identifiers (lacking links to other personal data) would require only opt-out consent options.
    - Facial detection and characterization systems that, as described, collect no personally identifiable information, do not require consent.
- Facial recognition applications should be held to standards that are fair and in line with consumer expectations, such as articulating the benefits and privacy practices to consumers and providing opportunities for consumers to make choices to mitigate or avoid risks.
    - Determine whether a proposed use is compatible with expectations by considering factors to include the context of collection; a reasonable awareness of how the data will be used; whether facial recognition is merely a feature of a product or service or integral to the service itself; and how the collection, use, or sharing of facial recognition data will likely impact the consumer.
    - Require consideration for how the use of facial recognition technology will impact both consumers who purposefully avail themselves of products or services which incorporate that technology as well as consumers who incidentally come into contact with these systems or cannot reasonably avoid a company's use of facial recognition technology.
    - Give special consideration to the age, sophistication, or degree of vulnerability of those individuals, such as children, in light of the purposes for which facial recognition technology is used, including whether additional levels of transparency, choice, and

data security are required. This includes awareness and compliance with any additional legal requirements that may apply.

- Require companies implementing facial recognition systems to develop and publish privacy policies describing their use of facial recognition systems in clear terms with a detailed description of the data collected. Privacy policies, educational help centers, and other materials are ways to ensure consumers and other stakeholders can understand the collection, use, retention, and appeal or deletion rights for individuals.
- Require data security practices and procedures commensurate with the sensitivity of the facial recognition data, the context in which facial recognition technology and facial recognition data is employed or used, the likelihood of harm to consumers, and other relevant factors. As with all personal data, provide data security appropriate to the sensitivity of facial recognition data when collected, shared, when at rest and in transit, and when used for research or product improvement purposes.

National Institute of Standards and Technology's Information Technology Laboratory Director Dr. Charles Romine stated that "NIST Interagency Report 8280, released on December 19, 2019, quantifies the effect of age, race, and sex on face recognition performance…[and] found empirical evidence for the existence of demographic differentials in face recognition algorithms that NIST evaluated." He asserted that "[t]he report distinguishes between false positive and false negative errors, and notes that the impacts of errors are application dependent…[and] I will first address one-to-one verification applications." Romine said that "[t]here, false positive differentials are much larger than for false negatives and exist across many, but not all, algorithms tested." He explained that "[a]cross demographics, false positives rates often vary by factors of 10 to beyond 100 times." Romine stated that "[f]alse negatives tend to be more algorithm-specific, and often vary by factors below 3."

Romine stated that "[f]alse positives might present a security concern to the system owner, as they may allow access to impostors…[and] [f]alse positives may also present privacy and civil rights and civil liberties concerns such as when matches result in additional questioning, surveillance, errors in benefit adjudication, or loss of liberty." He explained that "[f]alse positives are higher in women than in men and are higher in the elderly and the young compared to middle-aged adults…[and] [r]egarding race, we measured higher false positive rates in Asian and African American faces relative to those of Caucasians." Romine stated that "[t]here are also higher false positive rates in Native American, American Indian, Alaskan Indian and Pacific Islanders…[and] [t]hese effects apply to most algorithms, including those developed in Europe and the United States." He noted that "[h]owever, a notable exception was for some algorithms developed in Asian countries…[and] [t]here was no such dramatic difference in false positives in one-to-one matching between Asian and Caucasian faces for algorithms developed in Asia." Romine stated that "[w]hile the NIST study did not explore the relationship between cause and effect, one possible connection, and area for research, is the relationship between an algorithm's performance and the data used to train the algorithm itself."

Romine contended

> I will now comment on one-to-many search algorithms. Again, the impact of errors is application dependent. False positives in one-to-many search are particularly important because the consequences could include false accusations. For most algorithms, the NIST study measured higher false positives rates in women, African Americans, and particularly

in African American women. However, the study found that some one-to-many algorithms gave similar false positive rates across these specific demographics. Some of the most accurate algorithms fell into this group. This last point underscores one overall message of the report: Different algorithms perform differently. Indeed all of our FRVT reports note wide variations in recognition accuracy across algorithms, and an important result from the demographics study is that demographic effects are smaller with more accurate algorithms. A general takeaway from these studies is that, there is significant variance between the performance facial recognition algorithms, that is, some produce significantly fewer errors than others. Consequently, users, policy makers, and the public should not think of facial recognition as either always accurate or always error prone.

New York University's AI Now Institute Co-Founder and Co-Director Meredith Whittaker stated that she wanted to "five key points:

1. Facial recognition reflects and amplifies historical and present-day discrimination. Even if it were possible to make facial recognition accurate for everyone, ensuring accuracy does not address the social context in which it will be deployed, and will not reduce harms like abuse and discriminatory deployment. Facial recognition allows businesses and governments to intrude into people's lives without detection, and currently there are few guardrails to curtail biased and oppressive uses. Facial recognition is usually deployed by those who already have power – like employers, landlords, and police – to surveil and control those who have less power. Therefore, problems like racial profiling are likely to worsen with tools like facial recognition, especially as these technologies are disproportionately deployed to surveil Black communities, Latinx communities, and immigrant communities who already face systemic oppression and over-policing.
2. There is a blurry line between public and private facial recognition. Most facial recognition is developed and sold by private companies, regardless of whether governments or private actors are the end users. This means that we need to examine commercial systems and the incentive structures driving their development even in discussions that focus on government use. It also means that these technologies are shielded from accountability and oversight behind claims of corporate secrecy that make it difficult for the public and regulators to detect and redress harms.
3. Affect recognition and facial analysis pose particular dangers. In addition to problems with basic facial detection and identification, attempts to "recognize" emotions or "types" of people on the basis of facial expression lack any sound scientific support and further embed bias and discrimination within our society.
4. Standards and technical fixes are not enough to solve the problems with facial recognition. Standards for facial recognition assessment and auditing are a step in the right direction; however, such technical standards will not be sufficient to ensure that facial recognition is just or ethical. Further, narrow or weak standards run the risk of providing "checkbox certification," allowing vendors and companies to assert that their technology is safe and fair without accounting for how it will be used, or its fitness for a given context. If such standards are positioned as the sole check on facial recognition systems, they could function to obfuscate harm instead of mitigate it.
5. It is time to halt the use of facial recognition in sensitive social and political contexts, by both government and private actors. Facial recognition poses an existential threat to democracy and liberty, and fundamentally shifts the balance of power between those using facial recognition and the populations on whom it's applied. This is true both in government and commercial contexts. While auditing standards and transparency are necessary to

answer fundamental questions, they will not address these harms. It is urgent that lawmakers act to halt the use of facial recognition insensitive social and political domains until the risks are fully studied and adequate regulations that center the communities most affected are in place.

Senate Commerce Examines Tech Industries of the Future

Last week, the Senate Commerce, Science, and Transportation Committee held a hearing titled "Industries of the Future" to "examine how the United States can maintain its global economic edge in artificial intelligence (AI), advanced manufacturing, quantum information science, biotechnology, and developing the next generation of wireless networks and infrastructure…[including] research and development investments, regulatory changes, and workforce training needed to ensure continued economic growth and job creation in America."

In advance of the hearing, Chair Roger Wicker (R-MS) introduced the "Industries of the Future Act of 2020" along with Senators Cory Gardner (R-CO) Tammy Baldwin (D-WI) and Gary Peters (D-MI). Under the bill, within four months of enactment, the Office of Science and Technology Policy (OSTP) must "submit to Congress a report on research and development investments, infrastructure, and workforce development investments of the Federal Government that enable continued United States leadership in industries of the future" that must include:

- The federal government's current level of investment in the "industries of the future;"
- A plan to double investments in both AI and quantum information;
- A plan increase all other investments in the "industries of the future" to $10 billion a year by FY 2025;
- a plan to elicit private sector investment in coordination with increased federal spending; and
- Legislation to bring about all these plans

An "Industries of the Future Coordination Council" would be established to advise the OSTP on how to maximize federal and non-federal efforts to develop and realize the "industries of the future."

While there is no definition of the "industries of the future" likely for the reason that the drafters would not want to limit OSTP's remit given industries that may arise in the future, in the findings section, the bill identifies the following as examples: AI, quantum information science, biotechnology, next generation wireless networks, advanced manufacturing, and synthetic biology.

In his opening statement, Chair Roger Wicker (R-MS) said "[t]he focus of this hearing is on the federal government's role in promoting the advancement of emerging technologies that will revolutionize the global economy such as driverless cars, real-time language translation, and personalized medicine." He claimed that "AI, quantum information science, advanced manufacturing, and the next generation of wireless communications technology all promise to fuel American prosperity, improve quality of life, promote national security, and create jobs." Wicker said that "[i]nnovations in AI are changing the way we access information, diagnose and treat illnesses, grow our food, power our homes, travel, and manufacture and deliver new products." He contended that "American leadership in AI is critical to maintaining our economic and national security." Wicker stated that "[c]reating global standards to ensure AI systems are reliable, safe, fair, and accurate presents an ongoing challenge that our witnesses should discuss." He claimed that

"[a]dvances in new production methods enables the United States to retain and create jobs…[and] [l]ast year this committee reported the "Global Leadership in Advanced Manufacturing Act of 2019," (P.L. 116-92) which became law."

Wicker stated that "I hope our witnesses – at least some of them – address the implementation of this law and other ongoing and expected administration efforts to promote advanced manufacturing." He added that "[t]he prospects for quantum computing are exciting…[and] [a]dvancements in quantum science have significant implications for the US economy and national defense, including biotechnology, next-generation military applications, and cyber security systems." Wicker remarked that "[t]he committee would also benefit from an update on the implementation of the National Quantum Initiative Act, and to hear what more needs to be done on this issue…[and] [e]stablishing a strong, reliable, and secure communications network to support these Industries of the future is essential to realizing the economic and social promise of next-generation technologies." He asserted that "5G – the fifth generation of wireless communications technology – is expected to usher in a new era of connectivity that will support significantly faster broadband speeds and higher data capacities…[and] will be fundamental to advancing developments in AI, quantum computing, and other groundbreaking innovations." Wicker said "I expect our witnesses from the FCC will want to address those and other issues regarding the role of 5G networks in facilitating these applications."

Wicker contended that "[i]nvestments in basic and applied research, infrastructure, and education have made the United States the global leader in science and technology…[and] [t]hose investments have driven economic growth and competitiveness in the United States for decades." He said that "[t]his committee also is dedicated to promoting American leadership in emerging science and technology…[and] [t]his week, along with Senators [Tammy] Baldwin (D-WI), [Cory] Gardner (R-CO), and [Gary] Peters (D-MI), I introduced legislation directing the Administration to develop a plan to double the baseline investment in federal government Industries of the Future programs by 2022, and to increase civilian spending on Industries of the future to $10 billion by 2025."

Ranking Member Maria Cantwell (D-WA) said the hearing is about the industries of the future and expressed her belief that is happening every day in Washington state in areas like AI, quantum computing, 5G, advanced manufacturing, and energy. She stressed the need for the U.S. government to continue investing and noted the U.S.' traditional investment in cutting edge technologies which often resulted in U.S. companies and researchers leading the way in those particular areas. Cantwell said while other nations, particularly China, are investing billions of dollars in those areas, the U.S. must step up. In regard to 5G, she emphasized that the most important issue regarding this technology is that the world should unite in declaring that no technological standard should become the de facto regime if it allows. Government to use backdoors. Cantwell added the technology of the future must also protect users from threats like cybersecurity and invasion, and consequently the U.S. has a very loud voice other nations should heed.

Cantwell argued that if the U.S. does not commit to very robust investments in technology, it will fall behind and would face grave consequences, particularly on a security level. She stated the U.S. must balance its research and development (R&D) portfolio to focus on "game-changing" technologies, which is why she believes the development of AI and combatting deep-fake photos are such important issues. Cantwell said the University of Washington in partnership with Washington State are studying how technology will impact elections and society and how these

threats magnify challenges and importance to federal agencies like intelligence and law enforcement and our ability to detect these deep fakes. She asserted the importance of this issue because this era is already upon us and lauded "a coalition of people" who are seeking to stabilize the "free media" in the U.S. Cantwell cited a University of Oxford study that found up to 47% of jobs in the U.S. could be automated as AI advances – which, she noted, does not mean these projected job losses are all related to AI – and referenced a 2016 Obama White House report that suggests even with some increases in AI-related jobs, there will still be effects. Cantwell said he and Senator Todd Young (R-IN) had introduced the "Fundamentally Understanding The Usability and Realistic Evolution of Artificial Intelligence Act of 2017" (aka the FUTURE of Artificial Intelligence Act of 2017) (S.2217/H.4625) in the last Congress that would require analysis of the impacts of AI and better prepare the U.S. government for a policy response.

Under Secretary of Commerce for Standards and Technology and National Institute of Standards and Technology Director Walter Copan explained that "NIST's efforts in AI are focused along three primary areas of effort:

- First, NIST is addressing fundamental questions about the use of AI. NIST has launched an effort to convene the community around key concepts of trustworthy AI, seeking to develop ways to measure, define, and characterize concepts around the accuracy, reliability, privacy, robustness, and explainability of AI systems.
- Secondly, NIST is heavily engaged in using AI across its research portfolio in a host of areas including biometrics, advanced materials discovery, smart manufacturing systems, and the design and characterization of engineered biological systems as just a few examples. Additionally, the outputs of NIST research in general, especially in the terms of well-characterized data sets, as well as our work in advanced microelectronic systems, will help advance the field of AI. These tools will enable researchers to better train and understand AI systems, including the design and manufacture of next-generation hardware required to reliably and safely run AI systems.
- Finally, standards engagement is a key element of NIST's mission, and we are deeply involved in multiple standards development bodies around the world. We are working with industry, government, and academia to establish governing principles and develop standards and identify best practices for the design, construction, and use of AI systems. It is vitally important for the U.S. to have a strong, persuasive, and consistent voice with the relevant standards organizations around the world.

Copan said that "[t]he Administration's multifaceted 5G efforts are being led by Director Larry Kudlow of the National Economic Council, and within that framework, NIST is playing a vital role. " He said that "NIST's programs in advanced communications support secure, reliable, high-speed wireless, and wireline communications critical to U.S. economic competitiveness, safety, and security." He added that "NIST measurement science research and support for the development of standards accelerates the deployment of next-generation communication technologies that promise to be faster and more reliable, including fifth-generation wireless networks." Copan claimed that "[t]hese technologies will support self- driving cars, internet of things (IoT) applications, drones, and future AI systems…[and] NIST is committed to solving the measurement and deployment challenges of this fast-moving field to help the U.S. achieve and maintain global leadership in these areas, and also to help U.S. industry establish manufacturing capabilities needed for domestic market supply."

U.S. Chief Technology Officer Michael Kratsios stated that the Trump Administration has "identified four key pillars that underpin our efforts across AI, 5G, quantum information science (QIS),

biotechnology, and advanced manufacturing—fundamental research and development (R&D), workforce development, light-touch regulation, and international engagement:"

- The federal government has a central role in supporting research and development in areas where there is little or no commercial incentive. My colleagues here today representing the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) are integral to U.S. R&D efforts and have done incredible work on behalf of the American people—making sure taxpayer dollars are used as effectively as possible to improve R&D in the areas that need it the most. Thanks to the bipartisan efforts of this Committee, in December 2018 the President signed the National Quantum Initiative Act, which established a National Quantum Coordination Office and authorized robust funding for QIS R&D activities across the federal government. This includes investing in quantum consortia—research centers where industry, government, non-profits, and academia can come together to advance QIS. Further, in February of 2019, the President launched the American AI Initiative—the U.S. national strategy for AI—which includes R&D as its first area of emphasis.
- To build and prepare the American workforce of the future, the Trump Administration has placed important emphases on STEM education, Pell Grant reform, apprenticeships, and reskilling and upskilling opportunities. Through the National Council for the American Worker, we've partnered with private sector leaders to support the 21st century workforce.
- For American innovation to flourish, the federal government must remove barriers, streamline processes, and be careful to not impose burdensome or preemptive regulation. That's why the President has taken action to eliminate hurdles to 5G deployment and create opportunities to enable new types of commercial drone operations so that they can legally develop, test and deploy their innovations in America. As part of the American AI Initiative, the White House recently proposed regulatory guidance principles for AI technologies which reflect our values of freedom, human rights, and civil liberties, and created a plan for federal engagement in the development of AI technical standards.
- On the international stage we have worked with our global partners to advance R&D and innovation underpinned by shared values. Demonstrating our commitment, the United States joined our global partners in the Organisation for Economic Co-operation and Development (OECD) to reach consensus on international principles supporting the trustworthy development of AI. And just last month, the United States joined the Government of Japan in signing a cooperative research agreement to advance QIS and technology for economic, societal, and security benefits.

Federal Communications Commission Commissioner Jessica Rosenworcel offered the committee "three ideas" for planning for future industries:

- First, we need a plan to deploy 5G technology to everyone, everywhere in the United States. Right now, we don't have one. As a result, we risk falling behind our global peers in the next generation of wireless leadership.
- Second, we need a plan to invest in training for the jobs of the future. Across the board, we need to do more to prepare our workforce for digital change. We can start with developing the workforce we need to build 5G networks. In the near term, the United States will have to train another 20,000 tower climbers to help install 5G equipment. In the longer term, we will need many other workers for every layer of the 5G ecosystem. But the Department of Labor currently does not list 5G jobs as a priority for its registered apprenticeship programs. This is a problem—and we should fix it.

- Third, we need a plan for both device and network security. Our 5G future will feature billions and billions of connected devices in the internet of things. These connections will increase our effectiveness and efficiency. They will inform our choices about how to deploy capital and scarce resources in everything from manufacturing on the factory floor to predicting crop yields on the family farm.

NIST Privacy Framework Released

The National Institute of Standards and Technology (NIST) has released a final version of its Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management "to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy." NIST claimed "[t]he Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends, such as artificial intelligence and the Internet of Things." However, NIST is literally up front with the fact that the Privacy Framework is entirely voluntary as this disclaimer appears on the title page: "[t]he contents of this document do not have the force and effect of law and are not meant to bind the public in any way." Nonetheless, in the absence of a federal privacy statute or other Trump Administration action on privacy, this document could serve as a significant part of the federal government's de facto approach to privacy and could gain widespread acceptance and be used broadly by the private sector.

NIST explained that the Privacy Framework is aimed at all organizations dealing with privacy issues. NIST stated it "is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction...[and] [u]sing a common approach—adaptable to any organization's role(s) in the data processing ecosystem—the Privacy Framework's purpose is to help organizations manage privacy risks by:

- Taking privacy into account as they design and deploy systems, products, and services that affect individuals;
- Communicating about their privacy practices; and
- Encouraging cross-organizational workforce collaboration—for example, among executives, legal, and information technology (IT)—through the development of Profiles, selection of Tiers, and achievement of outcomes.

NIST stated that "[t]he Privacy Framework follows the structure of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to facilitate the use of both frameworks together...[because] the Privacy Framework is composed of three parts: Core, Profiles, and Implementation Tiers." NIST claimed that "[e]ach component reinforces privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities." NIST explained the structure of the Privacy Framework:

- The Core is a set of privacy protection activities and outcomes that allows for communicating prioritized privacy protection activities and outcomes across an organization from the executive level to the implementation/operations level. The Core is further divided into key Categories and Subcategories—which are discrete outcomes—for each Function.
- A Profile represents an organization's current privacy activities or desired outcomes. To develop a Profile, an organization can review all of the outcomes and activities in the Core to determine which are most important to focus on based on business or mission drivers, data

processing ecosystem role(s), types of data processing, and individuals' privacy needs. An organization can create or add Functions, Categories, and Subcategories as needed. Profiles can be used to identify opportunities for improving privacy posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). Profiles can be used to conduct self- assessments and to communicate within an organization or between organizations about how privacy risks are being managed.

- Implementation Tiers ("Tiers") provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed. When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices, the degree of integration of privacy risk into its enterprise risk management portfolio, its data processing ecosystem relationships, and its workforce composition and training program.

In terms of possible applications, NIST claimed "[t]he Privacy Framework can support organizations in:

- Building customers' 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;
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
- Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.

NIST claimed

> 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?" To account for the unique needs of an organization, use of the Privacy Framework is flexible, although it is designed to complement existing business and system development operations. The decision about how to apply it is left to the implementing organization. For example, an organization may already have robust privacy risk management processes, but may use the Core's five Functions as a streamlined way to analyze and articulate any gaps. Alternatively, an organization seeking to establish a privacy program can use the Core's Categories and Subcategories as a reference. Other organizations may compare Profiles or Tiers to align privacy risk management priorities across different roles in the data processing ecosystem. The variety of ways in which the Privacy Framework can be used by organizations should discourage the notion of "compliance with the Privacy Framework" as a uniform or externally referenceable concept.

NIST launched its "Privacy Framework: An Enterprise Risk Management Tool" through the release of a request for information (RFI) in November 2018 that led to the development and release for comment of a Privacy Framework discussion draft and thereafter engaged in extensive interaction with the private sector to shape the final document. While the Privacy Framework may stand as the

Administration's approach on privacy, this was to be but one part of the Administration's policy on privacy. The National Telecommunications and Information Administration's (NTIA) attempt to develop an "approach to consumer data privacy" has stalled. In September 2018, the 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" that was composed of two components: (1) A set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and (2) a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections. However, in the meantime, top NTIA officials stepped down, throwing into question the agency's focus on this initiative.

FTC Explains More Detailed Data Security Settlements

In a blog posting, the Federal Trade Commission's (FTC) Director of the Bureau of Consumer Protection Andrew Smith explained the recent evolution in how the agency crafts its data security settlements. In short, in light of a 2018 federal appeals court ruling against the FTC, the agency has been writing more detailed data security settlements that place additional responsibilities on companies subject to such orders in order to avoid legal challenges.

In 2018, the United States Court of Appeals for the Eleventh Circuit (Eleventh Circuit) ruled against the FTC's finding that claimed "that LabMD's data security practices were unreasonable and constitute an unfair act or practice that violated Section 5 of the Federal Trade Commission Act." The Eleventh Circuit held that the FTC's cease and desist order against LabMD was unenforceable because it did not enjoin a specific act or practice and instead required the company to revamp its information security regime without direction on how to do so. According to the Eleventh Circuit, the FTC lacks the power to stipulate companies implement reasonable data security standards because such commands are too vague and are therefore unenforceable for a company may never be sure of what will satisfy the FTC and any court empowered to oversee the settlement. Hence, the FTC may not direct companies to institute reasonable data security standards. The FTC chose not to appeal this case to the Supreme Court of the U.S., meaning there now exists a situation in which the use of a reasonableness standard in information security settlements would not be allowed in one part of the federal court system while still being allowed in the other ten circuits. The FTC has responded by crafting more detailed data security settlements.

In order to make this change in how the agency approaches settling data security cases, Smith listed the "three major changes that improve data security practices and provide greater deterrence, within the bounds of our existing authority:"

- First, the orders are more specific. They continue to require that the company implement a comprehensive, process-based data security program, and they require the company to implement specific safeguards to address the problems alleged in the complaint. Examples have included yearly employee training, access controls, monitoring systems for data security incidents, patch management systems, and encryption. These requirements not only make the FTC's expectations clearer to companies, but also improve order enforceability.
- Second, the orders increase third-party assessor accountability. We still rely on outside assessors to review the comprehensive data security program required by the orders, and now we require even more rigor in these assessments. For example, the orders clearly and specifically require assessors to identify evidence to support their conclusions, including independent sampling, employee interviews, and document review. The assessors must retain

documents related to the assessment, and cannot refuse to provide those documents to the FTC on the basis of certain privileges. When FTC staff can access working papers and other materials, they are better able to investigate compliance and enforce orders. Perhaps most importantly, our new orders give us the authority to approve and re-approve assessors every two years. If an assessor falls down on the job, we will withhold approval and force the company to hire a different assessor.

- Third, the orders elevate data security considerations to the C-Suite and Board level. For example, every year companies must now present their Board or similar governing body with their written information security program — and, notably, senior officers must now provide annual certifications of compliance to the FTC. This will force senior managers to gather detailed information about the company's information security program, so they can personally corroborate compliance with an order's key provisions each year. Requiring these kinds of certifications under oath has been an effective compliance mechanism under other legal regimes (e.g., securities law), and we expect it will likewise ensure better year-round governance and controls regarding FTC data security orders.

Smith listed five recent settlements that include these features: ClixSense (pay-to-click survey company), i-Dressup (online games for kids), DealerBuilt (car dealer software provider), D-Link (Internet-connected routers and cameras), Equifax (credit bureau), Retina-X (monitoring app), and Infotrax (service provider for multilevel marketers).

Finally, Congress could address the issues raised in the Eleventh Circuit case by including language in a privacy and data security bill giving the agency greater leeway in fashioning settlements and cease and desist orders.

White House Releases Draft AI Guidelines

The White House's Office of Science and Technology Policy (OSTP) has released a draft "Guidance for Regulation of Artificial Intelligence Applications," an Office of Management and Budget (OMB) memorandum that would be issued to federal agencies as directed by Executive Order (EO) 13859, "Maintaining American Leadership in Artificial Intelligence." However, this memorandum is not aimed at how federal agencies use and deploy artificial intelligence (AI) but rather it "sets out policy considerations that should guide, to the extent permitted by law, regulatory and non-regulatory oversight of AI applications developed and deployed outside of the Federal government." In short, if this draft is issued by OMB as written, federal agencies would need to adhere to the ten principles laid out in the document in regulating AI as part of their existing and future jurisdiction over the private sector. Not surprisingly, the Administration favors a light touch approach that should foster the growth of AI. OSTP is accepting comments on the draft for 60 days.

EO 13859 sets the AI policy of the government "to sustain and enhance the scientific, technological, and economic leadership position of the United States in AI." The EO directed OSTP along with other Administration offices, to craft this draft memorandum for comment. OSTP was to "issue a memorandum to the heads of all agencies that shall:

> (i) inform the development of regulatory and non-regulatory approaches by such agencies regarding technologies and industrial sectors that are either empowered or enabled by AI, and that advance American innovation while upholding civil liberties, privacy, and American values; and

> (ii) consider ways to reduce barriers to the use of AI technologies in order to promote their innovative application while protecting civil liberties, privacy, American values, and United States economic and national security.

Additionally, in a related step, as directed in the EO, "[w]ithin 180 days of the date of the memorandum...the heads of implementing agencies that also have regulatory authorities shall review their authorities relevant to applications of AI and shall submit to OMB plans to achieve consistency with the memorandum."

As a threshold matter, it bears note that this memorandum uses a definition of statute that is narrower then AI is being popularly discussed. OSTP explained that "[w]hile this Memorandum uses the definition of AI recently codified in statute, it focuses on "narrow" (also known as "weak") AI, which goes beyond advanced conventional computing to learn and perform domain-specific or specialized tasks by extracting information from data sets, or other structured or unstructured sources of information." Consequently, "[m]ore theoretical applications of "strong" or "general" AI—AI that may exhibit sentience or consciousness, can be applied to a wide variety of cross-domain activities and perform at the level of, or better than a human agent, or has the capacity to self-improve its general cognitive abilities similar to or beyond human capabilities—are beyond the scope of this Memorandum."

In terms of the practical effects of the draft memorandum, OMB would direct agencies to "avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth." OMB also direct agencies to use any Congressionally granted authority to regulate AI "in an area that may affect AI applications," agencies must take into account how any such regulation would affect AI growth and innovation. Moreover any risk assessments should measure the risks posed by AI as compared to the risks posed by the systems AI has been crafted to supplement or replace. Agencies must also account for how federal actions would affect state and local government action, but OMB would also direct agencies to consider using their authority "to address inconsistent, burdensome, and duplicative State laws that prevent the emergence of a national market." Finally, the memorandum makes clear "[w]here a uniform national standard for a specific aspect related to AI is not essential, however, agencies should consider forgoing regulatory action."

OSTP explained how the ten AI principles should be used:

> Consistent with law, agencies should take into consideration the following principles when formulating regulatory and non-regulatory approaches to the design, development, deployment, and operation of AI applications, both general and sector-specific. These principles, many of which are interrelated, reflect the goals and principles in Executive Order 13859. Agencies should calibrate approaches concerning these principles and consider case-specific factors to optimize net benefits. Given that many AI applications do not necessarily raise novel issues, these considerations also reflect longstanding Federal regulatory principles and practices that are relevant to promoting the innovative use of AI. Promoting innovation and growth of AI is a high priority of the United States government. Fostering innovation and growth through forbearing from new regulations may be appropriate. Agencies should consider new regulation only after they have reached the decision, in light of the foregoing section and other considerations, that Federal regulation is necessary.

OSTP listed the 10 AI principles agencies must in regulating AI in the private sector:

- Public trust in AI
- Public participation
- Scientific integrity and information quality
- Risk assessment and management
- Benefits and costs
- Flexibility
- Fairness and non-discrimination
- Disclosure and transparency
- Safety and security
- Interagency coordination

Chief Technology Officer (CTO) Michael Kratsios has been quarterbacking the Administration's approach on AI. During remarks to the media, he stated "[t]he U.S. AI regulatory principles provide official guidance and reduce uncertainty for innovators about how the federal government is approaching the regulation of artificial intelligence technologies...[and] [b]y providing this regulatory clarity, our intent is to remove impediments to private-sector AI innovation and growth." Deputy CTO Lynne Parker explained during the press rollout that "It's also important to note that these principles are intentionally high-level." She added that "[f]ederal agencies will implement the guidance in accordance with their sector-specific needs...[and] [w]e purposefully want to avoid top-down, one-size-fits-all blanket regulation, as AI-powered technologies reach across vastly different industries."

Finally, these AI principles follow a number of other, recent policy developments related to AI. In November, the National Security Commission on Artificial Intelligence (AI) has released its interim report and explained that "[b]etween now and the publication of our final report, the Commission will pursue answers to hard problems, develop concrete recommendations on "methods and means" to integrate AI into national security missions, and make itself available to Congress and the executive branch to inform evidence-based decisions about resources, policy, and strategy." The Commission released its initial report in July that laid out its work plan. Last summer, the National Institute of Standards and Technology (NIST) has released for comment the U.S. Leadership in AI: Plan for Federal Engagement in Developing Technical Standards and Related Tools and OSTP released the National AI Research & Development Strategic Plan: 2019 Update (AI R&D Plan). In late May, the Organization for Economic Cooperation and Development (OECD) adopted recommendations from the OECD Council on Artificial Intelligence (AI), and non-OECD members Argentina, Brazil, Colombia, Costa Rica, Peru and Romania also pledged to adhere to the recommendations. Moreover, the National Telecommunications and Information Administration (NTIA) signaled the Trump Administration's endorsement of the OECD effort.

GAO Issues Dim Assessment of Technology Modernization Fund

The Government Accountability Office (GAO) has released its first statutorily required assessment of the Technology Modernization Fund (TMF) and most notably found that based on the available data, none of the seven projects funded by the TMF are on track to show savings and there are administrative issues with how the Office of Management and Budget (OMB) and General Services Administration (GSA) are administering the program. The GAO found a host of problems with how costs are estimated, the data the TMF Board is asking for to decide on which projects to underwrite, the rate at which it is collecting fees from agencies to offset the costs of implementing the program,

and others. In short, this report is not a good selling point for the TMF and will likely not help the Administration makes its case for more funding in FY 2021.

The GAO must report every two years "on the TMF's status and on projects that have been awarded these funds." The GAO said that "[o]ur objectives were to: (1) determine the costs of establishing and overseeing the TMF, as compared to the savings realized by projects that have received awards; (2) assess the extent to which cost savings estimates for awarded projects are reliable; and (3) determine the extent to which agencies have used full and open competition for any acquisitions related to the awarded projects."

The GAO recounted that "[a]s of August 2019, the Technology Modernization Board had made seven TMF awards to five agencies, totaling about $89 million, and had transferred $37.65 million of this funding to the projects...[and] the General Services Administration (GSA) had obligated about $1.2 million to cover TMF operating expenses, but had recovered only about 3 percent of those expenses through fee payments." The GAO said that "[t]he seven projects are expected to make $1.2 million in scheduled fee payments by the end of fiscal year 2025; as of August, three projects have made fee payments totaling $33,165." The GAO allowed that "[b]ased on the current schedule, GSA will not fully recover these expenses until fiscal year 2025 at the earliest."

In terms of its finding, the GAO was not able to determine whether the seven projects had begun to realize cost savings. After obtaining cost estimates and project documentation from the five agencies, the GAO "confirmed that none of the seven projects had begun to realize cost savings; therefore, it was premature to compare projects' realized savings to TMF administrative costs." The agency further determined "[b]ased on our assessment of each project's cost estimate (used to derive the cost savings estimate) and the other measures we took to assess the reliability of the data included in the completed templates, we determined that the cost savings data for all seven TMF projects were not sufficiently reliable; thus, we did not include the estimated savings amounts in our report." Moreover, the administrative fees OMB and GSA projected to have collected from the agencies provided with TMF funds to offset the costs of setting up the program has been far short of projections. The GAO noted "[a]s of August 31, 2019, GSA's TMF Program Management Office had obligated about $1.2 million in operating costs for activities related to the establishment and oversight of the fund." The GAO stated that "[w]hile the office intended to assess administrative fees to fully recover its operating expenses, the actual amounts collected as of August 2019 had been less than planned." In fact, GSA had "collected $33,165 in administrative fees as of August 31, 2019." The GAO conceded that "[t]his was due to factors such as the office's formulation of fee rates based on appropriations levels that were higher than what was ultimately received, along with changes to several projects' scope and milestones." However, the GAO did find that "[a]s of August 31, 2019, six of the seven TMF-funded projects had awarded 23 contracts or task orders for work on the projects...[and] 22 of the 23 awards used full and open competitive procedures," thus satisfying one of Congress' directives in how OMB and GSA implemented the program.

Incidentally, the GAO did not entirely meet its legislative mandate. Even though Congress tasked the GAO with also reporting on "the number of IT procurement, development, and modernization programs, offices, and entities in the Federal Government, including 18F and the United States Digital Services, the roles, responsibilities, and goals of those programs and entities, and the extent to which they duplicate work," the agency did not address this in the report.

The GAO concluded that because the Board "has collected limited administrative fees to offset its

expenses" (i.e. the $1.2 million)...[it] has fewer funds than anticipated available to award to new projects." The GAO predicted that "[g]oing forward, OMB and the TMF Program Management Office are likely to face ongoing challenges in collecting administrative fees due to the factors that we have identified that affect fee collection and the office's lengthy time frame for recovering all costs." The GAO stated that "[w]hile OMB and the TMF Program Management Office are not currently on track to recover all operating expenses in a timely manner, Program Management Office officials have expressed the intent to revisit their fee structure, in part to address the lower than anticipated amount of fiscal year 2019 appropriations." The GAO stressed that "[b]ecause of the number of factors that are likely to affect fee collection, it will be critical that OMB and the TMF Program Management Office take steps to develop a plan that outlines the actions needed to fully recover TMF operating expenses with administrative fee collection in a timely manner in order to maximize the funds available for awards."

The GAO added that "since none of the seven TMF- funded projects' cost savings estimates can be considered reliable, it is not clear whether the projects receiving funding to date will save the government as much money as was estimated...[and] [a]n important aspect to the success of the TMF will be clarifying the established requirement that agencies follow Circular A-11's cost estimating process (that references GAO's cost estimating guidance discussed in this report) in order to help ensure that the reliability of estimated savings for awarded projects is improved."

The GAO made "five recommendations: two to OMB and three to GSA...[s]pecifically:

- The Director of OMB should develop and implement a plan with GSA that outlines the actions needed to fully recover the TMF Program Management Office's operating expenses with administrative fee collection in a timely manner. (Recommendation 1)
- The Director of OMB should work with GSA to clarify the requirement in the TMF guidance that agencies follow the cost estimating process outlined in Circular A-11 (that references GAO's cost estimating guidance discussed in this report), when developing the proposal cost estimate. (Recommendation 2)
- The Administrator of General Services should develop and implement a plan with OMB that outlines the actions needed to fully recover the TMF Program Management Office's operating expenses with administrative fee collection in a timely manner. (Recommendation 3)
- The Administrator of General Services should work with OMB to clarify the requirement in the TMF guidance that agencies follow the cost estimating process outlined in Circular A-11 (that references GAO's cost estimating guidance discussed in this report), when developing the proposal cost estimate. (Recommendation 4)
- The Administrator of General Services should develop detailed guidance for completing the Technology Modernization Fund project cost estimate template, including information on the data elements and the fields required to be completed, in order to help ensure the accuracy and completeness of the provided information. (Recommendation 5)"

Another Huawei/ZTE Final Interim Rule Issued

The Department of Defense has issued an interim final rule pursuant to language in the FY 2018 and 2019 National Defense Authorization Acts (NDAA) that requires the Pentagon and other federal agencies to stop buying or using telecommunications products and services from Huawei, ZTE, and other entities from China and Russia. Unlike the previously issued Huawei and ZTE rules, these regulations target only DOD procurements and then only those undertaken to fulfill the

department's "nuclear deterrence or homeland defense missions." Comments are due by January 17, 2020 for the drafting and issuing of a final rule.

In terms of the purpose and goal of the rule, the DOD claimed the rule "should increase security of systems and critical technology that is part of any system used to carry out the nuclear deterrence and homeland defense missions of DOD by prohibiting the use of telecommunications equipment or services from certain Chinese entities, including their subsidiaries and affiliates, and from any other entities that the Secretary of Defense reasonably believes to be owned or controlled by or otherwise connected to, the government of the People's Republic of China or the Russian Federation."

The rule defines the types of missions covered by this rule as

> (1) The nuclear deterrence mission of DOD, including with respect to nuclear command, control, and communications, integrated tactical warning and attack assessment, and continuity of Government; or
> (2) The homeland defense mission of DOD, including with respect to ballistic missile defense.

Moreover, the interim final rule introduces a new term: covered defense telecommunications equipment or services, which include:

> (1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities;
> (2) Telecommunications services provided by such entities or using such equipment; or
> (3) Telecommunications equipment or services produced or provided by an entity that the Secretary of Defense reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

The DOD explained the statutory bases for the interim final rule:

- Section 1656 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018 (Pub. L. 115-91) prohibited DOD from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service to carry out the DOD nuclear deterrence or homeland defense missions that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as a part of any system. Covered telecommunications equipment or services includes telecommunications equipment or services from certain Chinese entities, including their subsidiaries and affiliates, and from any other entities that the Secretary of Defense reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of the People's Republic of China or the Russian Federation.
- Likewise, section 889(a)(1)(A) of the NDAA for FY 2019 (Pub. L. 115-232) established a Governmentwide prohibition on procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as a part of any system. Covered telecommunications equipment or services includes certain video surveillance and telecommunications equipment or services from certain Chinese entities, including their subsidiaries and affiliates, and from any other entities that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of the People's Republic of China.

The DOD explained that this new "prohibition under 1656 differs from the Governmentwide prohibition under 889(a)(1)(A) in that it: Applies to equipment, systems, or services to carry out the DOD nuclear deterrence or homeland defense missions; includes different definitions of "covered telecommunications equipment or services" and "covered foreign country"; does not include exceptions from the prohibition; and provides independent waiver authority to the Secretary of Defense.

In mid-August 2019, as required by Section 889, the DOD, General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) released an interim rule that bars federal agencies from buying Huawei, ZTE, and related Chinese "equipment, system[s], or service[s] that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system" unless an exception allows the agency to disregard this general ban. This rule took effect on August 13 per the deadline set in the FY 2019 NDAA. It bears note that this interim rule is applicable to all contracts going forward and some solicitations offered and contracts signed before August 13. The agencies followed up with "a second interim rule amending the Federal Acquisition Regulation (FAR) to require offerors to represent annually whether they offer to the Government equipment, systems, or services that include covered telecommunications equipment or services."

House Energy and Commerce Floats A Privacy and Data Security Discussion Draft

As rumored, in mid-December, the House Energy and Commerce Committee has released its privacy discussion draft that is the result of a bipartisan effort led by Consumer Protection & Commerce Subcommittee Chair Jan Schakowsky (D-IL) and Ranking Member Cathy McMorris Rodgers (R-WA). The subcommittee is sharing this draft with stakeholders and is asking for feedback by January 24 according to media accounts. However, the discussion draft includes a number of key sections in brackets, indicating areas still under discussion, chief among them: state preemption and a private right of action – two sticking points that have bedeviled the crafting of bipartisan legislation thus far. Still, there seems to be broad agreement on much of the structure of a bill with the Federal Trade Commission (FTC) being the primary enforcer and being granted rulemaking authority to implement the new regime.

It bears mention that stakeholders have stressed this is a work in progress and are looking for input from interested parties, ideally in the hope that some of the impasses might be broken. According to *The Hill*, a committee spokesperson said

> Committee staff have circulated a bipartisan staff discussion draft of comprehensive federal privacy legislation. This draft seeks to protect consumers while also giving data collectors clear rules of the road. It reflects many months of hard work and close collaboration between Democratic and Republican Committee staff. We welcome input from all interested stakeholders and look forward to working with them going forward.

According to the same article, Chair Frank Pallone Jr. (D-NJ) said "[w]e're trying to...make it bipartisan and get Republicans...[and] [t]hat's part of what we're working on." McMorris Rodgers was quoted as explaining "[t]his staff draft is not a finished product but will serve as an important step in the process for us to solicit feedback and continue to negotiate a final bill." She added that

"I'm appreciative of the bipartisan staff work that has gone into this and am committed to continue working with Chair Schakowsky towards a bipartisan privacy bill."

Overall, this bill tracks with other major privacy and data security bills released over the last few months. The Federal Trade Commission (FTC) would be the agency charged with drafting regulations to flesh out the new regime and enforcing the new standards against those entities that allegedly violate the new rights consumers would be granted. On this latter component of the new federal scheme, consumers would receive many of the same rights they would under the bills the two bills released by the chair and ranking member of the Senate Commerce, Science, and Transportation Committee: the "United States Consumer Data Privacy Act of 2019" (CDPA) and the "Consumer Online Privacy Rights Act" (COPRA) (S.2968), including the need for covered entities to obtain express consent for a number of data processing activities and the requirement that they heed a person's desires regarding data correction, retention, and transparency.

In terms of the scope of the draft bill, entities covered by the new bill are those already subject to FTC jurisdiction plus common carriers and non-profits, meaning vast sectors of the U.S. economy would need to comply. However, those entities currently outside the FTC's purview would not need to adhere to the new regime, including but not limited to banks, credit unions, holding companies, health care entities, and others. Limiting the range of covered entities to just those currently subject to the FTC's current mandate may be a way of tackling the issue of how legislation addresses entities currently subject to privacy and data security laws and regulations like the "Financial Modernization Act of 1999" (P.L. 106-102) (aka Gramm-Leach-Bliley) and the "Health Insurance Portability and Accountability Act of 1996" (P.L. 104-191) (HIPAA). Other bills deem these entities in compliance with the new standards so long as a covered entity is compliant with its existing regime.

The presence of brackets throughout the definitions section indicates that Democrats and Republicans are still negotiating over a number of critical terms. Nonetheless, the definition of data subject to the bill's protections and proscriptions is "any information about an individual possessed by a covered entity that is linked or reasonably linkable to a specific individual [or consumer device;]" and is identified as "covered information." Not surprisingly, these are exceptions to what is "covered information:" 1) data and processing related to employment; 2) "deidentified information," another bracketed term; and 3) "information that is rendered unusable, unreadable, or indecipherable," which is meant to create a safe harbor for covered entities to either use encryption or some other method that makes a person's data unusable if breached.

Like a number of other bills, the bill adds a subset of covered information: "sensitive information." This term is in brackets and in the draft is defined as

- (i) health information; (a bracketed term)
- (ii) biometric information;
- (iii) precise geolocation information;
- (iv) social security numbers;
- (v) information concerning an individual's race, color, religion, national origin, sex, age, or disability; (a bracketed term)
- (v) the contents and parties to communications;
- (vii) audio and video recordings captured through a consumer device; (a bracketed term)
- (viii) online browsing history with respect to sensitive information; (a bracketed term) and

- (vi) financial information, including bank account numbers, credit card numbers, debit card numbers, or insurance policy numbers.

Incidentally, other definitions that are brackets include "information broker," "pseudonymized information," and "sell," indicating that there is ongoing definition on what these terms will cover and omit.

Covered entities would need to craft and make available an easily understood, machine-readable privacy policy so that people could understand how their covered information and sensitive information is being used and then be in a position to consent in a meaningful fashion. Also, the FTC would be able to bring actions against those entities that fail to honor their privacy policies as a violation of Section 5 of the FTC Act's bar on deceptive and unfair business practices. Nonetheless, this section tasks the FTC with promulgating regulations that "require each covered entity to establish and implement reasonable policies, practices, and procedures regarding the processing of covered information." Such privacy policies should contain:

- the categories of covered information that the covered entity processes;
- how and under what circumstances covered information is collected directly from the individual;
- the categories and the sources of any covered information processed by a covered entity that is not collected directly from the individual;
- a description of all of the purposes for which the covered entity processes covered information, including a number of detailed circumstances
- a description of how long and the circumstances under which the covered entity retains covered information;
- a description of all of the purposes for which the covered entity discloses covered information with processors, and, on a biennial basis, the categories of such processors;
- a description of whether and for what purposes the covered entity discloses information to third parties, and, on a biennial basis, the categories of such third parties;
- whether a covered entity sells or otherwise shares covered information with data brokers or processes covered information for targeted advertising;
- whether a covered entity collects covered information about individuals over time and across different websites or mobile applications when an individual uses the covered entity's website or mobile application;
- how individuals can exercise their rights to access, correct, and delete such individual's covered information as required under Section 5;
- how individuals can exercise their rights under Sections 6, 7, and 8, including how to modify and withdraw consent for the processing of covered information, and the consequences of exercising those rights;
- the effective date of the notice; and
- how the covered entity will communicate material changes of the privacy policy to individuals.

As noted in the itemized list above, each covered entity's privacy policy must describe all the purposes for which covered information is processed, and the bill lists specific categories of processing that must be disclosed. Firstly, the privacy policy must furnish a "detailed description" of all processing with "particularity" and if sensitive information is shared with third parties. Secondly,

covered entities must spell out how they customize their services and products based on data processing and how it prices these products or services differently based on data processing. Thirdly, the methods used to identify covered information must be disclosed if a covered entity uses any, including those used by its associated data processors and third parties. Finally, covered entities must tell individuals how they make decisions about people, and this might ultimately encompass consumer scores, but the term is bracketed.

Overall, this is a fairly detailed list of disclosures covered entities must make to individuals. However, like other legislation, it is possible and perhaps even likely that people confronted with such lists will grow inured to privacy policies and will simply click through to obtain the service or product they desire. Sure, the proactive individual would be able to determine when and how her privacy is being affected by a covered entity, but legislation that requires transparency of covered entities may not ultimately steer them away from some of the more objectionable practices in which they currently engage.

As noted, the privacy policy must "publicly available at all times and in a machine-readable format…in a manner that is clear, easily understood, and written in plain and concise language." Presumably, the machine-readable requirement would allow the FTC and state attorneys general would be able to easily amass and analyze these privacy policies if they have the technological capability to do so.

Large covered entities would need to meet heightened requirements related to their privacy policies even though there is disagreement apparently over the thresholds in annual revenue and the number of people whose information is processed that would need to be cleared before these requirements attach. Generally, "[e]ach covered entity that either has annual revenue in excess of [$250,000,000] in the prior year or that processes covered information of more than [10,000,000] individuals [or consumer devices] in the prior year, shall be required to submit to the [FTC], on an annual basis, a privacy filing." Note the brackets in the cited language. Nonetheless, wherever the bill ends up drawing the lines on revenue and processing, a subset of large covered entities would need to submit a "detailed and granular description" of all the aforementioned components of their privacy policies. Additionally, these large entities would need to do the same regarding all processing of categories of covered information the covered entity engages in. These entities would also need to disclose their data retention policies, a risk assessment of its data processing activities and measures taken to mitigate these risks, any material changes in privacy policies or practices, and description of any "security incidents under any federal or State law to individuals, a consumer reporting agency, or to a State attorney general or other State or federal government entity, and the results of all audits or investigations undertaken following any such security incidents."

Two other salient things to note about these filings. First, these annual reports would be posted on the FTC's website, which would throw extra light on these companies' data processing activities. Second, large entities would need to pay $15,000 per year with each filing, a figure that is bracketed in the bill but the FTC may adjust for inflation annually.

Obviously, such annual filings would provide the FTC with vastly greater insight into large technology companies like Facebook and Amazon but other swaths of the U.S. economy as many retailers, automakers, manufacturers, and others may well qualify for this enhanced oversight. Also, it may be possible the agency could launch investigations and possibly bring actions based on these filings.

The FTC would need to study how best to communicate privacy policies to people and then promulgate regulations that would require covered entities to use these methods for conveying some of the information that must be part of their privacy policies. This rulemaking would also articulate the "form and manner" by which covered entities must make their privacy policies available to individuals when information is first collected.

There are detailed limits on the processing of personal information obtained by a covered entity, and the FTC would be required to promulgate regulations fleshing them out. Generally, processing may not occur without the consent of a person but "[c]onsent for the processing of covered information is implied to the extent the processing is consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual." There is bracketed language on allowing people to opt out of first party marketing. However, for any data processing that is not consistent with a reasonable person's expectations would require affirmative, express consent, and the FTC would need to promulgate regulations to spell out what constitutes affirmative express consent. Certain data processing would be prohibited, principally obtaining consent under false pretenses. Some covered information may not be processed, subject to certain exceptions, including biometric information, health information, geolocation information, and other specified types.

The FTC would promulgate regulations that would spell out the requirements covered entities and processors must enshrine in agreements in disclosing and processing personal information. Moreover, "[a] covered entity shall not disclose covered information to a third party unless the covered entity obtains prior express, affirmative consent of the individual to whom the covered information pertains."

Individuals would receive a number of rights regarding how their data is collected, processed, and maintained. Firstly, a person could ask and receive an answer as to whether a covered entity is processing her information. In the same vein, a person could also access his personal information held by the covered entity, the categories of personal information processed, any sources from which this personal information was collected, and other details. People would have the right to correct personal information held by a covered entity. Entities with more than $250 million in revenue and that process the personal information of more than 10,000 people a year would need to meet additional requests. People could also ask a covered entity to delete covered information.

The bill limits data retention. Generally, "a covered entity shall not keep, retain, or otherwise store covered information for longer than is reasonably necessary for the purposes for which the covered information is processed" subject to a number of exceptions, including complying with legal requirements, for security purposes, preventing risks to health and safety, and other reasons.

A section titled "CHILDREN'S PRIVACY" contains no text other than "TBD," suggesting there is interest on the committee in folding more stringent provisions into the bill to strengthen the existing regime, the "Children's Online Privacy Protection Act" (COPPA) (P.L. 115-277).

The FTC will conduct a notice and comment rulemaking to set data security standards for covered entities. Within one year of enactment, the FTC "shall require each covered entity and processor to implement and maintain reasonable administrative, technical, and physical security measures, policies, practices, and procedures to protect and secure covered information against unauthorized

access and acquisition." These standards will be geared to the activities, sensitivity of the data being held and processed, the cost of implementing safeguards, and the current available safeguards. However, this legislative direction to the FTC is "limited to the provisions included in this section." In the event of a breach, a covered entity must notify the FTC and submit its security policies which shall be exempted from FOIA requests.

The bill bans take-it-or-leave consent arrangements or financial incentives for agreeing to data processing. Specifically, "[a] covered entity shall not condition the provision of a product or service or the quality of customer experience to any individual on an individual's agreement to waive any rights guaranteed by this Act [or to the individual's consent to the processing of the individual's covered information other than information necessary to provide the product or service]." Note the brackets in the original text, suggesting the final clause in the provision is subject to final negotiation. Likewise, a covered entity may not offer "a financial incentive in exchange for an individual's agreement to waive any rights guaranteed by this Act [or to the individual's consent to the processing of the individual's covered information other than information necessary to provide the product or service]."

The bill would make it unlawful "for any covered entity to process covered information…in a manner that discriminates against or makes an economic opportunity unavailable or offered on different terms, on the basis of a person's or class of persons' race, color, religion, national origin, sex, age, or disability" concerning a range of areas, including housing, employment, credit, insurance, and others. It shall also be unlawful "for a covered entity to process covered information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person's or class of persons' race, color, religion, national origin, sex, age, or disability." Additionally, the burden of proving such discrimination would be shifted to covered entities in that they would need to prove their processing is not discriminatory.

Smaller covered entities may be able to use "self-regulatory guidelines governing the processing of covered information by a covered entity" approved and monitored by the FTC. Eligible entities include those with $25 million or less in annual revenue, that process 50,000 or fewer people's personal information a year, and that derive 50% of less of their revenue from selling personal information. The FTC must approve any such guidelines before use and any future modifications and may withdraw approval if the guidelines no longer adhere to the Act.

Information brokers would need to identify themselves as such on their websites and register with the FTC.

The FTC would need to establish a Bureau of Privacy to enforce this Act and all other data security and privacy laws within the FTC's purview, including Section 5 of the FTC Act and COPPA. The FTC would be able to fine covered entities for violations in the first instance of up to more than $42,000 per violation. The FTC would be free to seek all the current relief it can under Section 5, including injunctions, restitution, disgorgement of ill-gotten gains, and other types of remedies. There is language in brackets that would cap civil penalties, but that would seem to be an item under discussion. State attorneys general would also be able to bring actions and seek all the relief the FTC can, and there is a subsection title in brackets, A Private Right of Action, with no provisions, which is not surprising given the opposition of Republicans to such a means of relief. Similarly, there is a title with no language regarding state preemption.

House Administration Hearing on Election Vendor Security

Two weeks ago, the House Administration Committee held its most recent hearing on election security but with a focus on the security practices and standards of the vendors contracting with states and localities to provide hardware and software for the conduct of elections.

Election security will likely continue to be a topic on the minds of cybersecurity policymakers. Moreover, while House and Senate Democrats will likely continue to push for the enactment of election security legislation, it is very unlikely that Senate Majority Leader Mitch McConnell (R-KY) would allow any bill favored by Democrats to come to the floor. In late October, the House took up and passed its third bill on election security in 2019, the "Stopping Harmful Interference in Elections for a Lasting Democracy Act" (SHIELD Act) (H.R. 4617), that addresses two of the technological facets of foreign disinformation campaigns aimed at U.S. elections according to the House Administration Committee's summary:

- Helps prevent foreign interference in future elections by improving transparency of online political advertisements.
    - Russia attempted to influence the 2016 presidential election by buying and placing political ads on platforms such as Facebook, Twitter and Google. The content and purchasers of those online advertisements were a mystery to the public because of outdated laws that have failed to keep up with evolving technology. The SHIELD Act takes steps to prevent hidden, foreign disinformation campaigns in our elections by ensuring that political ads sold online are covered by the same rules as ads sold on TV, radio, and satellite.
- Prohibits deceptive practices about voting procedures.
    - Independent experts have identified voter suppression tactics the Russians used on social media, including malicious misdirection designed to create confusion about voting rules. The SHIELD Act incorporates the Deceptive Practices and Voter Intimidation Prevention Act to prohibit anyone from providing false information about voting rules and qualifications for voting, provides mechanisms for disseminating correct information, and establishes strong penalties for voter intimidation.

In February 2019, the House passed "For The People Act of 2019" (H.R. 1) on a party-line vote, which included a process by which cybersecurity standards would be established for election infrastructure vendors and would also authorize grants for states and localities to upgrade and secure their election systems. For example, "qualified election infrastructure vendors" must agree "to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee" and to promptly report cybersecurity incidents to the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC).

In late June 2019, the House considered and passed the "Securing America's Federal Elections (SAFE) Act of 2019" (H.R. 2722) also largely along a party-line vote. In the Committee Report, the House Administration Committee explained the bill:

- H.R. 2722 provides critical resources to states and localities to bolster election infrastructure, including necessary funds to replace aging voting equipment with voter-verified paper ballot voting systems and implement additional cybersecurity protocols. The bill also helps states and localities plan for future elections by providing ongoing maintenance funding on

a biannual basis. The legislation provides grant programs for states to implement required risk-limiting audits, a best practice audit system that confirms election outcomes with a high degree of confidence.
- The legislation also institutes accountability for election technology vendors so that they abide by cybersecurity standards, including agreeing to report known or suspect security incidents involving election infrastructure.

In October, Senate Democrats tried to bring election security legislation to the floor despite the opposition of McConnell and other Republicans. On October 22, Amy Klobuchar (D-MN) and Senate Minority Whip Dick Durbin (D-IL) each asked for unanimous consent to bring up election security legislation, and they, too, were blocked by objections lodged by Republicans. Klobuchar wanted to bring forward her bill, "Honest Ads Act" (S. 1356), which, according to her press release upon introduction, "enhances the integrity of our democracy by improving disclosure requirements for online political advertisements by:

- Amending the Bipartisan Campaign Reform Act of 2002's definition of electioneering communication to include paid Internet and digital advertisements.
- Requiring digital platforms with at least 50,000,000 monthly viewers to maintain a public file of all electioneering communications purchased by a person or group who spends more than $500.00 total on ads published on their platform. The file would contain a digital copy of the advertisement, a description of the audience the advertisement targets, the number of views generated, the dates and times of publication, the rates charged, and the contact information of the purchaser.
- Requiring online platforms to make all reasonable efforts to ensure that foreign individuals and entities are not purchasing political advertisements in order to influence the American electorate."

Durbin's consent request to bring another Klobuchar bill, the "Election Security Act" (S. 1540), directly to the Senate floor was also blocked. Durbin claimed the bill "would provide critical resources to election officials through an initial $1 billion investment in our election infrastructure, followed by $175 million every 2 years for infrastructure maintenance…[and] would also require the use of voter-verified paper ballots, strengthen the Federal response to election interference, and establish accountability measures for election technology vendors."

On October 23, Senators Mark Warner (D-VA), Klobuchar, and Ron Wyden (D-OR) made unanimous consent requests to bring to the floor the following bills:

- The "Foreign Influence Reporting in Elections Act" (S. 2242)
- S. 2669, A bill to amend the Federal Election Campaign Act of 1971 to clarify the obligation to report acts of foreign election influence and require implementation of compliance and reporting systems by Federal campaigns to detect and report such acts, and for other purposes.
- The "Securing America's Federal Elections Act" (SAFE Act) (S. 2238)

However, Senator Marsha Blackburn (R-TN) objected to each request.

Chair Zoe Lofgren (D-CA) noted the committee's jurisdiction over federal elections and the hearing would help in discharging the committee's responsibilities as it would hear from the vendors of most of the U.S.'s systems. She claimed this was the first time the CEOs of the three major vendors have

appeared together at a Congressional hearing. Lofgren stated that the companies they lead provide at least 80% of the 350,000 voting machines currently being used, reaching over 100 million registered voters. She said despite the outsized role of these companies in the U.S.' democracy, some have accused these companies of obfuscating and misleading election administrators and the American public. Lofgren remarked that others have suggested there is an insufficient regulatory structure over this sector. She quoted a witness from a May 2019 hearing who argued there are more regulations governing ball point pens and magic markers than the nation's election systems, and consequently, there may be more work to do and more for Congress to learn about the industry.

Lofgren said many have concerns about voting systems with remote access software. She added that it would be wise to be sure that voting companies no longer sell machines that have network capabilities. Lofgren referenced a 2019 report in *Motherboard* that detailed a group of election security experts who discovered that the backend systems of systems in at least ten states were connected to the internet despite one company's claim its systems were not. She stated it is also important to understand supply chains. Lofgren mentioned a 2019 study by Interos that showed that 20% of the components in a popular voting machine came from Chinese companies and 59% of the suppliers in the company's supply chain had locations in either China or Russia.

Lofgren stated she has heard concerns about the control and ownership of voting machine companies, including the fact that all three of the major firms are privately held or owned by private equity firms. She declared that it is in Congress' interest to better understand who could benefit from the administration of U.S. elections. Lofgren asserted there are threats to U.S. infrastructure. She said Special Counsel Robert Mueller's report found that Russian intelligence operatives targeted employees of voting system companies and installed malware on the company's network. Lofgren noted that the Voluntary Voting Systems Guidelines have not been updated since 2005 and only minor changes were made in 2015. She asserted there is more to be done to bolster confidence in election systems and voting. Lofgren said that is why the House has acted by passing the "SAFE Act" (H.R. 2722) in June 2019 that would require individual, durable voter verified paper ballots, strict cybersecurity standards, risk limiting audits, that machines and systems not have internet and wireless connectivity, and accountability mechanisms for election technology vendors. She said the bill awaits consideration in the Senate.

Lofgren said that last month Congress appropriated $425 million to the states to improve election security that builds on the $380 million appropriated in 2018. She declared securing our elections should not be a partisan issue. Lofgren contended that election security is about upholding a democracy of, by, and for the people. She averred that democracy relies on everyone having their vote counted.

Ranking Member Rodney Davis (R-IL) stated he has been looking forward to this hearing for some time and that his priority as ranking member is to focus on non-partisan and effective oversight of the nation's elections, which are maintained by the states and not the federal government. He claimed that this does not means the committee and the House do not have important roles to play in oversight. Davis said the witnesses have state, county, and local jurisdictions as clients who know their electorate best. He added there are also witnesses with experience running those elections. Davis said that threats from foreign nations are not going away. He said the Senate Intelligence Committees report found that no votes were changed, no voting systems were manipulated, and no voter registration data were altered or deleted by Russia or any foreign actor. Davis cited former

Assistant Secretary of Homeland Security Jeanette Manfra's 2017 testimony in which she expressed confidence in the U.S. voting infrastructure because it is fundamentally resilient.

Davis said the committee has a responsibility to strengthen the relationship between states and the federal government to ensure that Americans' are and will continue to be protected. He allowed there has been some disagreement with Democrats on how best to accomplish this mission, but he stated his belief that the goal is the same. Davis said instead of getting into a debate on issues like paper vs electronic and federal vs state, the committee should focus on areas within the federal government's purview that need improvement and that may allow for bipartisan agreement. He stated the committee crafted and helped pass the "Help America Vote Act of 2002" (HAVA) that provided much needed funds to states so they could update their election security and voting infrastructure and created the Election Assistance Commission (EAC). He asserted that HAVA required the EAC to create a set of specifications and requirements against which voting systems can be tested, the Voluntary Voting Systems Guidelines. Davis said the EAC approved the VVSG in 2005, updated them in 2016, and is currently working on the next iteration. He called for the committee to hold a hearing on the EAC to examine the process by which the guidelines are crafted and other agency processes. Davis suggested that the committee should revisit HAVA as well for there are many areas of election systems not addressed by the law, including e-poll books and securing online registration databases. He argued that HAVA should be updated to create incentives for vendors to create a more secure election system.

Davis stated that Congress has taken recent steps to protect elections. Last month, the FY 2020 National Defense Authorization Act (NDAA) was enacted that contained a number of election security provisions, including provisions regarding the sharing of intelligence regarding election threats. He said similar provisions were in the election bill he introduced the "Election Security and Assistance Act" (H.R. 3412), including one that requires the Director of National Intelligence, in coordination with several agencies, to develop a strategy for countering Russian cyber-attacks against U.S. elections. Davis noted the $425 million provided by a FY 2020 appropriations bill to states, and territories to make general election improvements, including upgrades to election technology and security. He claimed much has been done but much remains to be done. Davis said the nation's elections should be secured without partisan politics.

Georgetown University Law Center Professor Matt Blaze offered "three central recommendations:

- Paperless (DRE) voting machines should be phased out from US elections immediately, and urgently replaced with precinct-counted optical scan ballots that leave a direct artifact of voters' choices.
- Statistically rigorous "risk limiting audits" should be routinely conducted after every election, in every jurisdiction, to detect and correct software failures and attacks.
- State and local voting officials should be provided significant additional resources, infrastructure, and training to help them protect their election management IT systems against increasingly sophisticated adversaries."

University of Florida Professor Dr. Juan Gilbert stated that "[i]n 2018, the National Academies of Science, Engineering and Medicine released a consensus report titled, "Securing the Vote: Protecting American Democracy" and "I would like to share some key recommendations:"

- Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine, using a ballot-marking device; they may be counted by hand or by machine, using an optical scanner. Recounts and audits should be conducted by human

inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing, for example, machines that do not produce a voter-verifiable paper audit trail, should be removed from service as soon as possible. Currently, there's no known way to secure a digital ballot. At this time, any election that is paperless is not secure. Therefore, Internet voting, specifically, the return of ballots should not be used at this time.

- Vendors and election officials should be required to report any detected efforts to probe, tamper with, or interfere with any election systems, including, voter registration systems.
- Each state should require a comprehensive system of post-election audits of processes and outcomes.
- A detailed set of cybersecurity best practices for state and local election officials should be continuously developed and maintained.
- Congress should provide funding to help state and local governments modernize their election systems and improve their cybersecurity capabilities. Congress should also authorize and provide funding for a major research initiative on voting.

Election Systems & Software President and CEO Tom Burt stated

> We strive for continuous improvement in all facets of our business, and we embrace our role as a leader in our industry. As I mentioned earlier, ES&S was the first provider to publicly state it will no longer sell a primary voting system that does not provide an auditable paper record. We strongly support post-election audits and believe that a true audit requires a physical paper record that can be both tabulated and subsequently audited. We support the EAC receiving the financial and administrative support needed from Congress to bolster the federal testing and certification program by conducting additional and more rigorous penetration testing of voting systems from all vendors who endeavor to service and support elections across America. This testing must become mandatory for elections providers and must be managed at the federal level with standards and testing methods that are applied evenly and diligently to equipment from all providers. Attached to this statement is a published op-ed I wrote that supports these suggested federal mandates.

Burt added

> Let me also be very clear that we do not believe we are perfect or invincible. On rare occasions, mistakes are made, a machine falters, or a human error is uncovered. Our reaction to any problems that occur is swift and comprehensive. Our record makes clear that working with the relevant local officials, we immediately seek to identify the potential problem, send in a team of experts to consult with the customer, and do everything possible to remedy the issue and ensure that final election results are reported accurately.

Brennan Center for Justice Counsel Liz Howard asserted "Congress has much work to do to further protect our election infrastructure in 2020 and beyond:

> A. Congress Should Conduct Meaningful Oversight Over Federal Funding for Election Security in 2020. First, it is critical that Congress provide meaningful direction and oversight over how the $805 million that Congress has allocated over the last two years to bolster state election security is used. Ongoing oversight efforts by this committee and others have had a substantive and positive impact on voting system security across the nation. As the committee continues these efforts throughout 2020, it should pay particular attention to the

measures that state and local election officials can implement to make our voting networks more resilient before 2020.

B. The Federal Government Should Enact Comprehensive Election Security Reform to Protect Elections in 2020 and Beyond, and this should include greater oversight of election system vendors. Next, Congress must enact comprehensive election security reform. This comprehensive reform will require consistent funding for election security, as proposed in bills such as the For the People Act and the SAFE Act. It will also require substantive vendor oversight. Currently, there are no federal laws or regulations requiring private vendors to take any action in the event of a cyberattack, or even to attest that they follow good security practices. Voting systems are subject to voluntary federal certification, but the vendors who supply, maintain, and often program those machines, along with integrated products such as electronic pollbooks, are not. Thus, although a vendor may sell federally certified voting systems, that certification process does not speak to vendor practices more generally that can affect, for example, the security of voters' personal information.

C. The Federal Government Should Provide Consistent and Reliable Election Security Funding. Finally, a lack of financial resources presents the most significant obstacle to election security improvements in local jurisdictions. Congress took an important first step in 2018 by allocating $380 million to states for election security activities, and recently committed an additional $425 million. But these one-time investments are not enough to address the significant problems facing election systems, nor to provide long-term stability for future elections. Senator Warner, Vice Chair of the Senate Intelligence Committee, observed last week, "additional money is no substitute for a permanent funding mechanism for securing and maintaining elections systems." As the Congressional Task Force on Election Security found and numerous national security and election officials have said, "Election security is national security." There is an ongoing need for federal funding to help protect our election infrastructure from foreign threats.

Election Assistance Commission Commissioner Donald Palmer claimed "[t]he addition of $425 million in HAVA grant funds with a 20% state match will go a long way toward enhancing election technology and improving security in state and local elections…[and] [s]imultaneously, the 40% increase in the Election Assistance Commission (EAC) budget will allow us to bolster existing programs and enhance resources." He noted "the EAC's distribution of $380 million in 2018 HAVA funds to states in the lead up to the 2018 midterms was, and continues to be, critically important to helping officials secure elections infrastructure."

Palmer highlighted "an important update to our Testing and Certification Program that occurred late last year…[and] the Testing and Certification Program Manual allowed for minor –or de minimis –software changes without the overhead of a full-blown voting system certification testing campaign." He said that "[o]ur goal is to be nimble as possible in working with manufacturers to quickly respond to a rapidly changing threat environment." Palmer stated that "in November of 2019, the EAC's Testing and Certification Program issued a Notice of Clarification providing clear guidelines on submitting these minor software changes for certification."

Palmer stated that "[t]remendous progress was also made in 2019 toward the adoption of Voluntary Voting System Guidelines (VVSG) 2.0…[that] represents a significant leap forward in defining standards that will serve as the template for the next generation of secure and accessible voting systems." He explained that "[t]he EAC Standards Board and the Board of Advisors will meet

in April 2020 to consider these new requirements…[and] [a]fter their key input, it is my hope that the VVSG 2.0 will be finalized and voted on over the upcoming months."

Second Draft of NIST IoT Cyber Guidance Released

The National Institute of Standards and Technology (NIST) has released its second draft of Interagency or Internal Report (NISTIR) 8259, "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline," developed so that "IoT device manufacturers will learn how they can help IoT device customers with cybersecurity risk management by carefully considering which device cybersecurity capabilities to design into their devices for customers to use in managing their cybersecurity risk." The first draft was released for comments in July 2019, and this is but one of the voluntary guides NIST has released on IoT. NIST explained that "[t]his second public draft contains the same main concepts as the initial public draft, but their presentation has been revised to clarify the concepts and address other comments from the public." Comments on this latest draft are due by February 7.

NIST stated that "[t]his second public draft of NISTIR 8259 describes activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers...[and] builds upon NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks." Like other NIST documents, this is not binding on private or public sector entities, but it will likely prove persuasive.

NIST stated that "[t]his document describes six voluntary, but recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers." NIST said that "[f]our of the six activities primarily impact decisions and actions performed by the manufacturer before a device is sent out for sale (pre-market), and the remaining two activities primarily impact decisions and actions performed by the manufacturer after device sale (post-market)." NIST stated that "[p]erforming all six activities can help manufacturers provide IoT devices that better support the cybersecurity-related efforts needed by IoT device customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised IoT devices."

NIST listed "Activities with Primarily Pre-Market Impact:

- Activity 1: Identify expected customers and define expected use cases. Identifying the expected customers and use cases for an IoT device early in its design is vital for determining which device cybersecurity capabilities the device should implement and how it should implement them.
- Activity 2: Research customer cybersecurity goals. Manufacturers cannot completely understand all of their customers' risk because every customer faces unique risks based on many factors. However, manufacturers can make their devices at least minimally securable by those they expect to be customers of their product who use them consistent with the expected use cases.
- Activity 3: Determine how to address customer goals. Manufacturers can determine how to address those goals by having their IoT devices provide particular device cybersecurity capabilities in order to help customers mitigate their cybersecurity risks. To provide manufacturers a starting point to use in identifying the necessary device cybersecurity capabilities, this document defines a core device cybersecurity capability baseline, which is a set of device cybersecurity capabilities that customers are likely to need:

    - Device Identification: The IoT device can be uniquely identified logically and physically.
    - Device Configuration: The configuration of the IoT device's software and firmware can be changed, and such changes can be performed by authorized entities only.
    - Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
    - Logical Access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
    - Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
    - Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.
- Activity 4: Plan for adequate support of customer goals. Manufacturers can help make their IoT devices more securable by appropriately provisioning device hardware, firmware, software, and business resources to support the desired device cybersecurity capabilities.

NIST detailed "Activities with Primarily Post-Market Impact:

- Activity 5: Define approaches for communicating to customers. Many customers will benefit from manufacturers communicating to them—or others acting on the customers' behalf, such as an internet service provider or a managed security services provider—more clearly about cybersecurity risks involving the IoT devices the manufacturers are currently selling or have already sold.
- Activity 6: Decide what to communicate to customers and how to communicate it. There are many potential considerations for what information a manufacturer communicates to customers for a particular IoT product and how that information will be communicated. Examples of topics are:
    - Cybersecurity risk-related assumptions that the manufacturer made when designing and developing the device
    - Support and lifespan expectations
    - Device cybersecurity capabilities that the device provides, as well as cybersecurity functions that can be provided by a related device or a manufacturer service or system
    - Device composition and capabilities, such as information about the device's software, firmware, hardware, services, functions, and data types
    - Software and firmware updates
    - Device retirement options

Although the recommendations in this and other NIST reports are not binding on federal agencies, federal contractors, or other private entities, it is quite likely that NIST's cachet could result in this and other IoT documents setting a de facto standard for IoT security and possibly be folded into federal legislation. For example, the "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668/S. 734) calls on NIST to complete its work on its IoT guidance documents and then use them as the basis for recommendations to the Office of Management and Budget (OMB) to form the federal approach to requiring federal IoT meet certain security standards. Both committees of jurisdiction in the House and Senate have reported out their versions of this bill, opening the possibility that the attached document and NISTIR 8228 could ultimately drive IoT cybersecurity in the federal government and in the private sector.

Moreover, a few weeks ago, the Senate passed the "Developing Innovation and Growing the Internet of Things Act" (DIGIT Act) (S. 1611) a few days after California and Oregon laws came into effect to regulate the security of the Internet of Things (IoT). And, while the DIGIT Act would not preempt or affect the two new state statutes, it would establish the beginnings of a statutory regime for the regulation of IoT at the federal level. According to the Committee Report, "the DIGIT Act, would do the following:

- Help create a national strategy for IoT.
- Require the Secretary of Commerce (Secretary) to convene a working group of Federal agencies, advised by a steering committee of nongovernmental stakeholders established within the Department of Commerce (DOC), to provide recommendations to Congress on how to plan and encourage the growth of IoT.
- Direct the Federal Communications Commission (FCC), in consultation with DOC's National Telecommunications and Information Administration (NTIA), to issue a report (after seeking public comment) on the spectrum needs required to support IoT.

However, most crucially, under the DIGIT Act, the IoT working group submits its findings and recommendations to Congress regarding the regulation of IoT within 18 months of enactment. Presumably this report could form the basis for follow on legislation to take a more direct hand in regulating IoT or could inform how executive branch agencies approach regulation.

The House has not yet taken up legislation like the DIGIT Act.

In California, SB 327 "would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." As noted, this bill took effect on January 1, 2020. Oregon's HB 2395 also took effect on January 1 and would require IoT manufacturers "equip a connected device with reasonable security features."

Further Reading

- "'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020" – *The New York Times*. Not surprisingly U.S. and western officials expect a cyber onslaught during the 2020 election. However, they also expect new players on the field and new methods to disrupt and influence the election. But of greatest concern, many states, localities, and private sector entities throughout the election system are woefully unprepared. Some claim many systems are not poised to address the tactics used by the Russians in 2016 let alone some of the new attacks being seen.
- "The Secretive Company That Might End Privacy as We Know It" – *The New York Times*. By scraping sites like Facebook and using an artificial intelligence algorithm, a company has pioneered a technology that is currently being used to allow law enforcement agencies to identify people from photographs by matching them from publicly available pictures on the internet. The privacy implications from this breakthrough are still being grappled with.
- "Many companies are not taking the California Consumer Privacy Act seriously—the attorney general needs to act" – *Consumer Reports*. A number of companies are openly planning to defy the consumer provisions in the California Consumer Privacy Act. Given

public statements by the California Attorney General's office about only being able to bring a handful of cases a year, if companies are actually intending to not comply with the privacy statute.

- "Iran can use cyberattacks against the U.S. That's not nearly as bad as it sounds." And "Get ready for serious cyberattacks from Iran, experts say" – *Washington Post*. One expert downplays the risks posed by Iranian retaliatory cyberattacks given their capability and the limited impact of most cyberattacks while other experts predict imminent and possibly dire attacks from Iran.
- "'Online and vulnerable': Experts find nearly three dozen U.S. voting systems connected to internet" – *NBC News*. Despite the federal government and vendors claiming that no voting or lection systems are connected to the internet, and advocacy organization finds more than 35 systems have wireless systems protected only by firewalls that can be breached fairly easily.
- "Hackers Are Breaking Directly Into Telecom Companies to Take Over Customer Phone Numbers" – *Motherboard*. Entrepreneurial hackers have moved beyond SIM swapping and are instead targeting telecom employees to hack directly into their systems to achieve the same goal of compromising phones.