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

Spotlight: A Privacy Bill A Week

Last week, we examined the "Data Care Act" (S. 3744), a bill introduced at the tail end of the last Congress by Senator Brian Schatz (D-HI) and other Senate Democrats as a marker of where they stood on data privacy issues. This bill built on a concept fleshed out by law professor Jack Balkin in his article "Information Fiduciaries and the First Amendment" that would place duties on companies collecting and using consumer data similar to those that lawyers and doctors must meet in how they handle client and patient information. Balkin explained that these so-called "information fiduciaries" should "have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."

Schatz has been in negotiations with other members of the Senate Commerce, Science, and Transportation Committee with the goal of developing a bipartisan bill to regulate privacy at a federal level. As discussed in past issues of the Technology Policy Update, stakeholders in both the House and Senate continue to negotiate privacy bills but significant disagreements have been reported regarding whether such a bill has a private right of action, preempts the "California Consumer Privacy Act" (CCPA) (A.B. 375) and other state laws, and whether a new regime is primarily enhanced notice and consent or certain conduct would no longer be allowed amongst other issues.

Nonetheless, for this week, let's examine a House bill, the "Information Transparency & Personal Data Control Act" (H.R. 2013) which is sponsored by Suzan DelBene (D-WA) and cosponsored by 22 other House Democrats. DelBene worked in Washington state's technology sector before transitioning to public service, including a stint with Microsoft. At present, this is not a bipartisan bill and consequently may be viewed as one of the House Democratic bills released this Congress.

Generally, this bill would require that all data "controllers" must secure opt-in consent from consumers to collect, use, share, or sell their "sensitive personal information" subject to significant exceptions. Controllers would need top draft and publish their data usage, security, and privacy plans, and then be audited annually by independent, third-parties. The Federal Trade Commission (FTC) would implement and oversee this new regime with state attorneys general being able to bring enforcement actions if the FTC does not act. Controllers who violate the new standards would be subject to enforcement including fines in the first instance and injunctive and equitable remedies under the FTC Act.

In terms of who would be part of the new privacy regulation scheme, the bill sweeps fairly wide. A "controller" is defined as "a person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information." The bill would explicitly pull "common carriers" (i.e. telecommunications companies) into the FTC's jurisdiction. Common carriers are normally subject to the jurisdiction of the Federal Communications Commission in regards to privacy. However, because common carriers are explicitly named as being part of the FTC's jurisdiction, that would suggest that other entities not usually under the agency's jurisdiction would not be subject to this bill (e.g. non-profits). Would entities all over the world that qualify as

controllers or processors be subject to the FTC's enforcement powers the way U.S. firms are subject to the General Data Privacy Regulation (GDPR)? It would seem so.

Also, the FTC would have jurisdiction over "processors" who are people "that process[] data on behalf of the controller," meaning that data brokers may get swept into the new privacy protection regulatory regime. However, it is not immediately clear if a data broker would be considered a controller or a processor. And finally, unlike some proposed data security bills, there is no carve out for entities subject to and in compliance with existing federal data security and privacy regimes like HIPAA and Gramm-Leach-Bliley.

In terms of implementation, like many other privacy bills, the FTC would be required to promulgate regulations within one year under the Administrative Procedure Act (i.e. notice and comment rulemaking) instead of the lengthier Moss-Magnuson procedures the agency usually must use. These regulations would put in place the requirements that controllers and processors of data would need to meet, including obtaining opt-in consent from consumers before their data could be collected and shared. As a general matter, consumers would need to opt-into the use and sharing of their "sensitive personal information" but they would need to opt-out of such practices if they pertain to "non-sensitive personal information." The dividing line between the two types of information would be crucial, and the bill provides broad categories of information that would qualify as "sensitive personal information." The FTC will undoubtedly need to flesh out some of the categories of "sensitive personal information" such as "health information," "genetic information," "biometric information," and other terms.

Likewise, the FTC will need to grapple with the term "information related to employment," which is one of the categories of non-sensitive personal information controllers would not need opt-in consent to collect, share, and use. It is easy to see how this term may overlap with some categories of sensitive personal information such as health information, Social Security number, financial account information, genetic information, and/or biometric information amongst others. This discussion of non-sensitive personal information also must mention another significant exception: "de-identified information (or the process of transforming personal data so that it is not directly relatable to an identified or identifiable consumer)." This provision seems to provide an incentive to controllers to de-identify sensitive personal information to the extent possible so that it is protected in the event of unauthorized access of acquisition but also so that it may be subject to the lesser requirements due for handling and using non-sensitive personal information. Presumably encrypting sensitive personal information would result in it being de-identified, for properly encrypted data could not be traced back to an identified or identifiable consumer. The bill is not entirely clear, and the FTC may well see the need to fill this gap when it promulgates regulations to effectuate this provision if it is enacted.

The FTC would also be charged with enforcing the new regime, but state attorneys general would also be empowered to bring enforcement actions in certain situations. Notably, state attorneys general could bring actions in the event the FTC does not act regarding alleged violations. However, state attorneys general would not be able to seek the full range of remedies available to the FTC and would instead only be able "to obtain appropriate injunctive relief," which may be temporary and permanent injunctions, disgorgement, restitution, rescission, and other such relief. But, a recent Seventh Circuit case (see article below) may cause the sponsors to broaden this term to all equitable relief to ensure that all such remedies may be sought.

In addition to controllers needing to get consumers to opt-in for some types of data collection and sharing, they would also need to "[p]rovide users with an up-to-date, transparent privacy, security, and data use policy that meets general requirements" including being "concise and intelligible," "clear and prominent in appearance," and "uses clear and plain language." This policy would also need to include the following, among other information:

- The "[i]dentity and contact information of the entity collecting the sensitive personal information.
- [T]he purpose or use for collecting, storing, processing, selling, sharing, or otherwise using the sensitive personal information.
- Third parties with whom the sensitive personal information will be shared and for what purposes.
- How consent to collecting, storing, processing, selling, sharing, or otherwise using the sensitive personal information, including sharing with third parties, may be withdrawn.
- What kind of sensitive personal information is collected and shared.
- Whether the sensitive personal information will be used to create profiles about users and whether they will be integrated across platforms.
- How sensitive personal information is protected from unauthorized access or acquisition.

Presumably the failure of a controller to comply with its own privacy, security, and data use policy could result in the FTC or a state attorney general bringing an action for unfair or deceptive practices under the FTC Act.

The exceptions are significant and depending on how the FTC construes these in regulation could determine how stringent or permissive the new data privacy regime would be. Despite the seemingly robust opt-in and transparency requirements, there are some significant exceptions to the general rule that consumers must opt-in before controllers may collect and share their sensitive personal information, namely:

> (A) Preventing or detecting fraud, identity theft, or criminal activity.
> (B) The use of such information to identify errors that impair functionality or otherwise enhancing or maintaining the availability of the services or information systems of the controller for authorized access and use.
> (C) Protecting the vital interests of the consumer or another natural person.
> (D) Responding in good faith to valid legal process or providing information as otherwise required or authorized by law.
> (E) Monitoring or enforcing agreements between the controller and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity.
> (F) Protecting the property, services, or information systems of the controller against unauthorized access or use.
> (G) Advancing a substantial public interest, including archival purposes, scientific or historical research, and public health, if such processing does not create a significant risk of harm to consumers.

Yet, the most significant exception may be in section (b)(2), which I'll quote in full: "[t]he [FTC] regulations promulgated pursuant to subsection (a) with respect to the requirement to provide opt-in consent shall not apply to the processing, storage, and collection of sensitive personal information or behavioral data in which such processing does not deviate from purposes consistent with a controller's relationship with users as understood by the reasonable user." Consequently, for the consumer using their Gmail account, any of Google's processing of sensitive personal information

may not be considered a deviation "from purposes consistent with a controller's relationship with users as understood by the reasonable user." The same may also apply to the current practices of Apple, Yahoo!, Microsoft, Amazon, etc. Not only would this represent a huge carve out to the exception that consumers must opt-in after receiving clear and easy to understand notice of what data is being collected, shared, and processed, with who, and for what purposes, it would seem to advantage those controllers already operating in the marketplace for they would not need to give consumers the choice of whether to opt-in.

Controllers of sensitive personal data would need a "qualified, objective, independent third-party" to conduct an annual "privacy audit," and then the controller would need to reveal publicly if it is in compliance. There may be issues related to the incentive structure in that these third-parties will be competing for the business of data controllers and may be inclined to slant their audit towards compliance for the sake of client management. Perhaps the bill would benefit from some of the measures enacted under Sarbanes-Oxley to weaken the incentives for auditors to water down their audits. Another issue may be that these audits do not need to be submitted to the FTC or state attorneys general until one of these regulatory officials makes known to the controller "allegations that a violation of this Act or any regulation issued under this Act has been committed by the controller." From a compliance standpoint, submitting all audits to the FTC in the same way companies must submit financial information to the Securities and Exchange Commission (SEC) would allow the FTC to have a better sense of compliance with its regulations, flag early any industry-wide trends or problems, or, yes, take enforcement action against non-compliant controllers. Of course such a system would be generally less attractive to data controllers. Finally, audits would not be necessary for small businesses for controller with the sensitive personal information of less than 5,000 people, and no audits would be necessary for non-sensitive information.

In terms of preempting state laws like the CCPA, this bill takes a seeming middle path. H.R. 2013 would preempt state laws "to the degree the law is focused on the reduction of privacy risk through the regulation of the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information." However, this preemption applies only to controllers subject to this bill. In what may prove important language, any controllers outside the scope of this bill would find themselves subject to state laws on privacy. Moreover, any state laws on processors would not be preempted by H.R. 2013, meaning entities like data brokers may still be subject to the CCPA, for example.

And, yet, this bill would seem to create some sunlight for states to add privacy and data security requirements above the federal floor created by this bill. To wit, the bill provides that "[a]ny private contract based on a State law that requires a party to provide additional or greater privacy for sensitive personal information or data security protections to an individual than this Act" would not be preempted. Therefore, in statute a state could make reference to H.R. 2013 as enacted and then require controllers and processors operating in those states to provide additional privacy or data security measures above and beyond those in FTC regulations.

The FTC would be directed to hire "50 new full-time employees to focus on privacy and data security, 15 of which shall have technology expertise," and appropriations of $35 million would authorized for the FTC "for issues related to privacy and data security." Of course, appropriators would then have to actually appropriate these funds before the FTC ever saw an additional dollar. And, to contextualize this funding increase, the House's FY 2020 bill that funds the FTC would provide the agency with $349.7 million, so the "Information Transparency & Personal Data Control

Act" would increase the agency's funding by roughly 10% above the House's preferred FY 2020 funding level and by a slightly higher percentage compared to FY 2019 funding for the FTC.

Seventh Circuit Rules Against FTC's Use Of Injunction Powers To Seek Restitution

A federal appeals court has ruled that the Federal Trade Commission (FTC) may not seek and obtain restitution for violations under its most common route of seeking this type of monetary damages. The U.S. Court of Appeals for the Seventh Circuit (Seventh Circuit) held that 15 U.S.C. § 53(b) permits the FTC to seek and obtain injunctions for ongoing and imminent harm in violation of statute, but the FTC does not have the authority to seek restitution (i.e. monetary damages based on part harm) under this section. The Seventh Circuit's ruling could ultimately limit the FTC's ability to seek to force entities to settle in the case of alleged poor data security or a breach, among other possible situations, and therefore the agency may have one less weapon with which to be the U.S.'s de facto data security protection authority. Alternatively, restitution may still be sought but under two other more involved routes.

In this case, *FTC v. Credit Bureau Center, LLC*, the Seventh Circuit explained the facts of the case:

> Michael Brown is the sole owner and operator of Credit Bureau Center, a credit-monitoring service. (We refer to both collectively as "Brown.") Brown's websites used what's known as a "negative option feature" to attract customers. The websites offered a "free credit report and score" while obscuring a key detail in much smaller text: that applying for this "free" information automatically enrolled customers in an unspecified $29.94 monthly "membership" subscription. The subscription was for Brown's credit-monitoring service, but customers learned this information only when he sent them a letter after they were automatically enrolled. Brown's most successful con- tractor capitalized on the confusion by posting Craigslist advertisements for fake rental properties and telling applicants to get a "free" credit score from Brown's websites.
>
> The Federal Trade Commission eventually took notice," sued Brown in federal court, and "[t]he judge entered a permanent injunction and ordered Brown to pay more than $5 million in restitution to the Commission."

While Brown lost on almost all his grounds for appeal, the Seventh Circuit agreed with the him that the federal trial court erred in allowing the FTC to recover restitution in tandem with an injunction. As the Seventh Circuit explained, 15 U.S.C. § 53(b) "authorizes only restraining orders and injunctions...[b]ut the Commission has long viewed it as also authorizing awards of restitution." The Seventh Circuit added that it had endorsed this view in a 1989 case, but subsequent Supreme Court cases had thrown into question such expansive readings of agency power that was not supported by statute. Moreover, the Seventh Circuit pointed out the FTC Act "has two detailed remedial provisions that expressly authorize restitution if the Commission follows certain procedures." Ultimately, the Seventh Circuit held that the "permanent-injunction provision [in 15 U.S.C. § 53(b)] does not authorize monetary relief."

Bigger picture, there is now a split between the Seventh Circuit and other federal appeals courts on whether the FTC can seek restitution under 15 U.S.C. § 53(b) when it seeks an injunction; the other circuits still allow the agency to do so. Often when there are splits in circuits, the Supreme Court will hear the case to settle these disputes. It remains to be seen whether the FTC will appeal to the Supreme Court in the hopes of reversing the Seventh Circuit. Of course, the FTC faces the risk the

Supreme Court agrees with the Seventh Circuit, and then its power to seek restitution in most federal courts is definitely removed. Additionally, there have been two other recent cases that have further refined the FTC's authority to police data security under Section 5 of the FTC Act. In 2015, in *FTC v. Wyndham Worldwide Corporation*, the Third Circuit upheld the FTC's ability to punish businesses for shoddy cybersecurity under Section 5, but in 2018, in *LabMD v. FTC*, the Eleventh Circuit ruled against the FTC's use of its authority to ban unfair and deceptive practices to compel an entity to institute data security practices under an unenforceable standard of "reasonableness."

Showing that the Seventh Circuit's reading of the FTC's authority may be too controversial for other circuits to adopt is the strongly worded dissent in which three circuit judges asserted "no court has ever tied the hands of a government agency in the way that the majority has done here, and the majority cites none." They added that "[n]othing whatever [in 15 U.S.C. § 53(b)] deletes from the list of possible affirmative acts that an injunction may include an order requiring the enjoined party to return ill-go en gains, or to pay money into a court escrow account, or otherwise to turn over property...[and] [t]hat should be enough by itself to show the error in the path the majority has taken."

Of course, Congress could always address the Seventh Circuit's ruling in a privacy or data security bill and essentially reverse the court by explicitly writing into statute that the FTC may also seek restitution when seeking an injunction under 15 U.S.C. § 53(b). However, whether this occurs remains to be seen.

Democratic Presidential Candidate Calls For Greater Broadband Access

Senator Elizabeth Warren (D-MA) wrote an op-ed for the *Washington Post* in which she discussed "plan for a new public option for broadband Internet, carried out by a new Office of Broadband Access that would manage an $85 billion federal grant program." Warren added that "[o]nly electricity and telephone cooperatives, nonprofit organizations, tribes, cities, counties and other state subdivisions would be eligible for grants." She noted that "a staggering 21.3 million Americans don't have access to high-speed broadband — no doubt an underestimate given the notorious loopholes in Federal Communications Commission (FCC) reporting requirements. This is despite more than a decade of efforts by policymakers at the state and federal level to end the "digital divide" and deliver universal access to high-speed Internet."

Warren claimed that the persistent digital divide "isn't an accident." She said "[b]lame Internet service providers (ISPs), such as Verizon, Comcast, AT&T and Charter, which have maximized their profits at the expense of rural towns, cities, low-income communities and communities of color across the country." Warren claimed that "[t]hese companies have deliberately restricted competition, kept prices high and used their armies of lobbyists to persuade state legislatures to ban towns and cities from building their own public networks…[and] the federal government has shoveled more than a billion in taxpayer dollars per year to private ISPs to expand broadband to remote areas, but these providers have done the bare minimum with these resources."

Warren claimed that "ISPs have been able to get away with fostering pseudo-monopolies because they spend a lot of money to keep the regulatory environment and the conversation surrounding it murky." She said that "FCC Chairman Ajit Pai, a former Verizon lawyer, has been an effective agent for ISPs…[and] led the charge to dismantle net neutrality last year, and he has done everything in his power to stop municipalities from building their own broadband infrastructure."

She asserted that "[h]e also attempted to gut the FCC's Lifeline program, one of the few tools the federal government has to provide Internet to low-income consumers."

In "My Plan to Invest in Rural America," Warren declared that "I will make sure every home in America has a fiber broadband connection at a price families can afford…[and] [t]hat means publicly-owned and operated networks — and no giant ISPs running away with taxpayer dollars." She explained that her plan will:

- **Make it clear in federal statute that municipalities have the right to build their own broadband networks.** Many small towns and rural areas have turned to municipal networks to provide broadband access in places that the private market has failed to serve — but today, as many as 26 states have passed laws hindering or banning municipalities from building their own broadband infrastructure to protect the interests of giant telecom companies. We will preempt these laws and return this power to local governments.
- **Create an Office of Broadband Access in my Department of Economic Development that will manage a new $85 billion federal grant program to massively expand broadband access across the country.** Under my plan, only electricity and telephone cooperatives, non-profit organizations, tribes, cities, counties, and other state subdivisions will be eligible for grants from this fund — and all grants will be used to build the fiber infrastructure necessary to bring high-speed broadband to unserved areas, underserved areas, or areas with minimal competition. The federal government will pay 90 cents on the dollar for construction under these grants. In exchange, applicants will be required to offer high-speed public broadband directly to every home in their application area. Applicants will have to offer at least one plan with 100 Mbps/ 100 Mbps speeds and one discount internet plan for low-income customers with a prepaid feature or a low monthly rate. Of these funds, **$5 billion will be set aside specifically for 100% federal grants to tribal nations to expand broadband access on Native American lands.** In addition to necessary "last mile" infrastructure, tribes will be able to apply for funds to build the missing 8,000 miles of middle mile fiber on tribal lands.
- **Appoint FCC Commissioners who will restore net neutrality.** I will appoint FCC Commissioners who will restore net neutrality, regulating internet service providers as "common carriers" and maintaining open access to the Internet. And I will require all telecommunications services to contribute fairly into the Universal Service Fund to shore up essential universal service programs that provide subsidies to low-income individuals, schools, and libraries to increase broadband adoption, including signing into law and building on the Tribal Connect Act, so that we can work toward every tribal library having broadband access.
- **Bolster the FCC's Office of Native Affairs and Policy.** This office holds trainings, technical assistance, and consultations for Indian Country. Providing it with dedicated, increased funding to expand its capacity will help close the digital divide.
- **Improve the accuracy of broadband maps.** Weak FCC oversight has allowed ISPs to greatly exaggerate how many households they serve and has given ISPs added fuel to downplay their failures and protect themselves from regulation. To provide universal broadband access and crack down on anti-competitive behaviors, the government has to know how extensive the problems are. I will appoint FCC Commissioners who will require ISPs to report service and speeds down to the household level, as well as aggregate pricing data, and work with community stakeholders — including tribal nations — to make sure we get this process right. Then, we will make these data available to the public and conduct regular audits to ensure accurate reporting.

- **Prohibit the range of sneaky maneuvers giant private providers use to unfairly squeeze out competition, hold governments hostage, and drive up prices.** It's time to crack down on all the anti-competitive behaviors that giant ISPs have used to steamroll the competition. We will return control of utility poles and conduits to cities, prohibit landlords from making side deals with private ISPs to limit choices in their properties, and ban companies from limiting access to wires inside buildings. We will make sure that all new buildings are fiber-ready so that any network can deliver service there, and we will also enact "Dig Once" policies to require that conduit is laid anytime the ground is opened for a public infrastructure project.
- **Ensure every person has the skills to fully participate in our online economy.** Even when there's access to broadband internet — and even when it's available at an affordable price — people may still not take advantage of it because they don't know how to use it. That's why I will work to pass the Digital Equity Act, which invests $2.5 billion over ten years to help states develop digital equity plans and launch digital inclusion projects.

Warren stated that "[t] here is both a moral and an economic imperative to enact a public option for broadband…[and] [i]f we stay on our current trajectory, ISPs will continue to decide which communities succeed and which ones fail." She stated that "[w]e imperil the success of future generations, threaten our competitiveness on the global stage and risk further diaspora from towns and cities that are in dire need of economic turnaround." Warren asserted that "[p]roviding universal, public access to broadband won't be easy." Warren stated that "[t]he ISPs aren't interested in competition and will fight to keep the status quo…[b]ut this is a worthy cause." She said that "[t]ogether we can change outcomes for forgotten towns and cities across our country."

The FCC responded to Warren's column with a statement:

> Under Chairman Pai's leadership of the FCC, the digital divide has been closing, average Internet speeds have substantially increased, and we've seen fiber deployed to more homes in a single year than any previous year in American history. Chairman Pai has also instituted innovative reforms to the Commission's universal service programs that are expanding broadband deployment across rural America in a cost-efficient manner. Indeed, the Commission just approved $4.9 billion last week for rural broadband deployment.

Administration Reportedly Changes Course and Asks Congress To Reauthorize Section 215 of the PATRIOT Act

Two separate media accounts have reported that the Trump Administration may have reversed course on a controversial provision allowing for the bulk collection of telephony metadata under the Foreign Intelligence Surveillance Act (FISA). Earlier this year, there were indications that the federal government had shut down the Section 215 program that had been exposed by former National Security Agency (NSA) contractor Edward Snowden due to technical problems in how the NSA and telecommunications companies were collecting these call records under the most recent reauthorization of these authorities, the USA FREEDOM Act of 2015 (P.L. 114-23). However, the Trump Administration is now asking that Congress reauthorize Section 215 along with three other provisions all of which expire in December. Moreover, the White House is asking for permanent extensions, something Congress has been loath to grant to the previous two Administrations.

In an August letter sent before he stepped down, former DNI Dan Coats asked the Senate Intelligence and Judiciary Committees for "the permanent reauthorization of the provisions of the

USA FREEDOM Act of 2015 that are currently set to expire in December…[that] provide the IC with key national security authorities."

Coats explained that "[t]he USA FREEDOM Act reauthorized three important, long-standing national security authorities:"

- First, the acquisition of so-called traditional business records under Title V of the FISA, which applies to tangible things relevant to authorized national security investigations.
- Second, the "roving wiretap" authority, which allows the government to effectively collect intelligence on a target who seeks to thwart surveillance by, for example cycling through cell phones.
- Third, the "lonewolf" authority, which allows the government to target certain non-U.S. persons engaged in international terrorism or activities in preparation there for.

Coats claimed that "[t]hese commonsense authorities are analogous to what is available in criminal investigations, have no history of abuse after more than 18 years, and should be reauthorized without sunset."

Coats added

> In addition, the Act banned bulk collection under a number of authorities and established a mechanism for the government to obtain pursuant to Title V of FISA certain telephone metadata records from U.S. telecommunications providers to help identify contacts of suspected terrorists. That mechanism applies to certain business records referred to as "call detail records," but not to the content of telephone calls. The National Security Agency has suspended the call detail records program that uses this authority and deleted the call detail records acquired under this authority. This decision was made after balancing the program's relative intelligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes.

Coats stated that "[h]owever, as technology changes, our adversaries' tradecraft and communications habits will continue to evolve and adapt…[and] [i]n light of this dynamic environment, the Administration supports reauthorization of this provision as well."

The House Judiciary Committee has reportedly started drafting a bill to reauthorize the FISA provisions on business records, roving wiretaps, and the lonewolf language currently in use. However, the committee has not been working on extending the power for NSA to vacuum up telephony metadata. The committee would need to take up the bill this fall as would other committees of jurisdiction in the House and Senate regarding portions of the program under their purview. It is possible that this reauthorization once again serves to block any other cybersecurity-related legislation as it did in 2015 for the bill that ultimately created the federal government's information sharing system under the "Cybersecurity Act of 2015" (P.L. 114-113).

Also in mid-August, more than 30 privacy and civil liberties advocacy organizations sent a letter to the House Judiciary Committee urging them "to ensure that any legislation that would reauthorize Section 215 of the USAPATRIOT Act contains critical reforms including, as one of several essential reforms, repealing the government's statutory authority to operate the Call Detail Records (CDR) program." They also urged the committee "to oppose, and our organizations will oppose, any bill to reauthorize Section 215 that does not include meaningful surveillance reforms…[and] [g]iven the

CDR program's extraordinary breadth, its lack of demonstrated efficacy, and the government's failure to lawfully implement it, repealing the CDR program is a necessary first step, although not sufficient without other major reforms."

Earlier this year, sparing began over the December expiration of FISA authorities used by U.S. intelligence agencies for surveillance of electronic communications. In early March, 30 progressive civil liberties and privacy groups sent a letter to House Democratic Leadership, asking them not to reauthorize three provisions in the "USA PATRIOT Act" (P.L. 107-56) that expire on December 15, 2019, including Section 215 the NSA has used to collect bulk telephone metadata among other communications. They stated "[w]e implore you to use the sunset of Section 215 as an opportunity to diminish rather than expand or extend the ability of Donald Trump and subsequent administrations to conduct mass surveillance of innocent people."

They stated

> More than five years have passed since the public became aware of the damning extent of mass surveillance that is conducted against innocent people in the United States pursuant to Section 215. Despite broad public outrage and several Congressional attempts to meaningfully reform Section 215, mass surveillance of innocent people continues. Indeed, one sub-provision of Section 215 created when the USA FREEDOM Act last extended this provision's sunset produced over 534 million call detail records in 2017, pursuant to only 40 orders. There are an additional 77 Section 215 orders from 2017, which have produced an unknown volume of additional records.

The letter was sent a few days after the *New York Times* quoted a top aide to House Minority Leader Kevin McCarthy (R-CA) in an article, claiming that the NSA is no longer using authority under the FISA that was exposed by former NSA contractor Edward Snowden. McCarthy's national security adviser Luke Murry made these claims during a *Lawfare* podcast.

In January 2018, Congress extended for six years Title VII of FISA that allows U.S. intelligence agencies to surveil non-U.S. persons outside the U.S. without a warrant and for non-intentional surveillance of U.S. persons reasonably believed to be outside the U.S. According to critics, the bill also allowed federal law enforcement and intelligence agencies to continue to conduct warrantless searches of communications acquired by the NSA in all cases except criminal investigations and authorized so- called "about" searches that would expand the scope of communications that could be examined.

Trump Administration Releases FY 2021 R&D Priorities

The Office of Budget and Management (OMB) and the Office of Science and Technology Policy (OSTP) have released the Trump Administration's FY 2021 Administration Research and Development (R&D) Budget Priorities, a memorandum for departments and agency heads to heed in drafting their FY 2021 budget requests. However, given how late in the year this memorandum has been released, it is not clear how much it will influence the budget process as the FY 2021 budget requests have been under preparation for some time. In recent years, the White House has released its R&D priorities in June of each year. Not surprisingly, the Administration is linking its R&D priorities to its larger policy goals and existing initiatives, including ensuring the national security of the U.S. and fostering U.S. dominance in current R&D such as cybersecurity,

semiconductors, and supply chain but in cutting edge fields like artificial intelligence and quantum computing.

OMB and OSTP claimed that "America's rise as the global leader in science and technology (S&T) began shortly after World War II, during which the Federal Government began investing significantly in basic and applied research, infrastructure, and education across many disciplines." The agencies stated that "[f]rom then until now- during America's First Bold Era in S&T- these Federal investments helped create a massive, multisector American S&T enterprise consisting of Federal agencies, world-leading colleges and universities, private industry, non-profit organizations, and Federal and National Laboratories."

The agencies stated that "[t]he resulting extraordinary discoveries and innovations laid the foundation for today's Second Bold Era in S&T – one characterized by unprecedented knowledge, access to data and computing resources, ubiquitous and instant communication, and technologies that allow us to peer into the inner workings of atomic particles as well as the vastness of the universe." OMB and OSTP noted that "[u]nfortunately, this Second Bold Era also features new and extraordinary threats which must be confronted thoughtfully and effectively."

OMB and OSTP declared

> The Trump Administration is firmly committed to continuing American S&T leadership in the Second Bold Era. Success will depend, in large part, on our ability to leverage- in entirely new and creative partnership and collaborative frameworks- the multisector S&T enterprise that emerged during the First Bold Era. It will depend upon striking a balance between the openness of our research ecosystem and the protection of our ideas and research outcomes. It will depend upon ensuring that our research environments are diverse, safe, inclusive, and accommodating as well as free from unnecessary administrative burdens. Success will depend upon ensuring that research is conducted with integrity and respect, which are foundational not only to the research process, but to the trust placed in the research enterprise by American taxpayers and reflective of America's values.

The agencies stated that "{t]his Fiscal Year 2021 (FY2021) R&D Budget Priorities memorandum provides direction to enable this Second Bold Era as part of a longer-term, multisector, national strategy to advance bold, transformational leaps in S&T, build a diverse workforce of the future, solve previously intractable grand challenges, and ensure America remains the global S&T leader for generations to come." OMB and OSTP explained that "[f]or FY2021, the five R&D budgetary priorities in this memorandum ensure that America remains at the forefront of scientific progress, national and economic security, and personal well being, while continuing to serve as the standard-bearer for today's emerging technologies and Industries of the Future." The agencies asserted that "[t]his memorandum also describes five high-priority crosscutting actions that span all five R&D budgetary priorities and require departments and agencies to coordinate, collaborate, and partner with one another and with the other sectors of the S&T enterprise to maximize success."

OMB and OSTP identified their five R&D budgetary priorities, and we've included some of the narrative language relating to key initiatives.

1. American Security

- Advanced Military Capabilities: Relevant departments and agencies should invest in R&D to deliver the advanced military capabilities that will help meet emerging threats and protect American security into the future, including offensive and defensive hypersonic

weapons capabilities, resilient national security space systems, and modernized and flexible strategic and nonstrategic nuclear deterrent capabilities.

- Critical Infrastructure Resilience: Departments and agencies should invest in critical infrastructure R&D that improves resilience to natural disasters and physical threats, including extreme terrestrial events, cyber and electromagnetic pulse attacks, and exploitation o f supply chain vulnerabilities.
- Superconductors: Departments and agencies, working in collaboration with industry and academic partners where appropriate, should prioritize investments that will enable whole of government access to trusted and assured microelectronics for future computing and storage paradigms, consistent with the Executive Order on Securing the Information and Communications Technology and Services Supply Chain.
- Critical Minerals: The Executive Order on a Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals identifies innovation and R&D as key to reducing vulnerabilities and building supply chain resilience for rare earths and critical minerals. Priorities include developing recycling and reprocessing technologies, identifying substitute materials, and developing new and improved processes for critical mineral extraction, separation, refining, and alloying.

2. American Leadership in Industries of the Future

- Artificial Intelligence, Quantum Information Science, and Computing: Departments and agencies should prioritize basic and applied research investments that are consistent with the 2019 Executive Order on Maintaining American Leadership in Artificial Intelligence and the eight strategies detailed in the 2019 update of the National Artificial Intelligence Research and Development Strategic Plan. Consistent with the 2018 National Quantum Initiative Act and the 2018 National Defense Authorization Act, departments and agencies should prioritize R&D advancing fundamental QIS, building and strengthening the workforce, engaging industry, and providing infrastructure supporting QIS while coordinating relevant activities to ensure intelligence,defense,and civilian efforts grow synergistically. In terms of computing, departments and agencies should work together to explore new applications in and support R&D for high performance future computing paradigms, fabrication, devices, and architectures alongside sustainable and interoperable software; data maintenance and curation; and appropriate security.
- Advanced Communications Networks and Autonomy: Departments and agencies should support the development and deployment of advanced communications networks by prioritizing R&D consistent with the National Spectrum R&D Strategy. They should prioritize R&D to lower barriers to the deployment of surface, air, and marine autonomous vehicles with a focus on developing operating standards, integration approaches, traffic management systems, and defense/security operations. Departments and agencies should prioritize R&D that enables electric vertical-takeoff-and-landing and civil supersonic aircraft, including for type certification, the creation of over-land supersonic flight noise standards, and low-sonic-boom aircraft research.

3. American Energy and Environmental Leadership

- Advancing energy technologies, understanding our unexplored ocean and expanding use of ocean data, and improving our Earth system prediction capabilities are Administration priorities that will enhance the nation's economic vitality, national security, and environmental quality.

4. American Health & Bioeconomic Innovation

- American medical and biotechnology breakthroughs have enhanced the quality and longevity of life for countless people around the world. The Trump Administration continues to focus R&D on key research breakthroughs and solutions that improve the health of our veterans and individuals of all ages, while enabling new opportunities in the Bioeconomy.

5. American Space Exploration and Commercialization

- R&D investments should continue to leverage efforts underway at American universities and in the private sector and focus on ensuring American leadership in space by supporting the Trump Administration's call for a return of Americans to the Moon's surface by 2024 and utilizing the Moon as a proving-ground for a future human mission to Mars.

The Administration identified its "PRIORITY CROSSCUTTING ACTIONS:"

1. Build and Leverage a Diverse, Highly Skilled American Workforce

- The Trump Administration's 2018 report, Charting a Course for Success: America's Strategy for STEM Education (STEM Strategy), articulates a vision that "all Americans will have lifelong access to high quality STEM education and the United States will be the global leader in STEM literacy, innovation, and employment." Achieving this vision depends on a multisector seamless STEM education and training ecosystem that can meet the needs of all Americans from all backgrounds and ZIP codes and can adapt to the changing, and often growing, demands for STEM knowledge and skills in both the workplace and in everyday life.

2. Create and Support Research Environments that Reflect American Values

- To advance S&T progress and ensure maximum return on taxpayer investment in R&D, the laboratory, the factory, the field, and any other setting where R&D is performed must welcome all individuals without prejudice and enable them to work safely, efficiently, ethically, and with respect, consistent with the American values of free inquiry, competition, openness, and fairness. Four high-priority areas related to research environments require significant attention:
  - Reducing administrative burdens on Federally-funded research;
  - Improving rigor and integrity in research;
  - Creating safe and inclusive research environments; and
  - Protecting American research assets.

3. Support Transformative Research of High Risk and Potentially High Reward

- Many of the greatest advances in S&T- for example, the first direct detection of gravitational waves-can be traced to Federal support of R&D that is intellectually challenging but has the potential to transform society in profound and positive ways. In order to remain the world leader in S&T, America must continue to support bold thinking and potentially transformative research ideas.

4. Leverage the Power of Data

- The President's Management Agenda (PMA) Cross-Agency Priority (CAP) Goal 2, "Leveraging Data as a Strategic Asset," describes three objectives: develop along-term, enterprise-wide Federal Data Strategy to better govern and leverage the Federal Government's data; enable Government data to be accessible and useful for the American public, businesses, and researchers; and improve the use of data for decision-making and accountability for the U.S. Government, including for policy-making, innovation, oversight, and learning. Department and agency investments should reflect and support the objectives

of CAP Goal 2 and the Federal Data Strategy framework. Priorities include improving data accessibility and security, leveraging AI and other emerging technologies, and building a data-skilled workforce. Departments and agencies should coordinate and collaborate with each other and with the private sector and nonprofits to leverage data and data tools, consistent with all applicable laws and regulations governing data use and sharing.

5. Build, Strengthen, and Expand Strategic Multisector Partnerships

- Partnerships between and among R&D departments and agencies, academic institutions, established and startup businesses, nonprofit institutions, and others involved in the U.S. S&T enterprise are instrumental to building and leveraging our Nation's innovation capacity and lie at the core of success for the Second Bold Era of S&T.

Since the OMB Circular A-11 for the upcoming budget cycle sets September 9 as the deadline for initial agency FY 2021 budget submissions, it is an open question on the extent to which departments and agencies will be able to comply with or incorporate this R&D budget guidance. What may occur is that ongoing or already planned initiatives may get dressed up in the language of the Administration's FY 2021 R&D priorities in these initial budget plans, and then OMB works with agencies to refine or change their budget submissions this fall.

Of course, when this memorandum is read alongside the Trump Administration's current and previous budget proposals, the White House can be seen as stepping on the gas and the brake at the same time given the deep cuts in R&D they have proposed. As the Congressional Research Service (CRS) explained, the Administration's "budget request for FY2020 includes approximately $134.1 billion for R&D," but "most federal agencies would see their R&D funding decline" with the exception being the Department of Defense.

CRS added:

> Among the agencies with the largest proposed reductions in R&D funding in the FY2020 budget compared to the FY2018 actual levels are the Department of Energy ($2.8 billion, 15.8%), the National Science Foundation ($567 million, 9.0%), and National Aeronautics and Space Administration ($475 million, 4.0%). The President's FY2020 budget request would reduce funding for basic research by $1.5 billion (4.0%), applied research by $4.3 billion (10.5%), and facilities and equipment by $0.5 billion (12.8%), while increasing funding for development by $4.5 billion (8.3%).

Administration officials would likely claim they are merely cutting away funding that does not align with their policy goals and is therefore superfluous. Besides the White House must know Congress will not go along with R&D cuts such as these and will appropriate dollars either at the current funding level at a slight increase.

NIST Identifies OMB As Reason For Backlog

The National Institute of Standards and Technology (NIST) took the unusual step of posting a public update on pending significant Special Publications (SP) and Federal Information Processing Standard (FIPS) documents essentially pointing the finger at the Office of Management and Budget (OMB) for the delay in the publication of final versions. In the below notice posted on NIST's Computer Security Resource Center website, NIST explained that it "is not updating our publication dates due to a review cycle being incorporated by the Office of Management and Budget, Office

of Information and Regulatory Affairs (OIRA)," OMB's gatekeeper for many regulatory actions. NIST added that seven of the nine pending documents depend on OIRA green-lighting the release of NIST Special Publication 800-53, Revision 5 (Final Public Draft), Security and Privacy Controls for Information Systems and Organizations. Also, unlike the SPs that are almost always not binding on agencies and private sector entities but are highly respected and persuasive, the hold up at OIRA is blocking the issuance of two revised Federal Information Processing Standard (FIPS) documents that are mandatory for most federal agencies and their contractors.

NIST released a draft of SP 800-53 Rev. 5 in August 2017 and explained that it anticipated "producing the final draft of this publication in October 2017 and publishing the final version not later than December 29, 2017," meaning that NIST's timeline for issuance of this document has slipped by more than 18 months. In the draft SP 800-53, NIST asserted that "[t]here is an urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure—ensuring those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States.: NIST claimed that its revised SP 800-53 "responds to the call by the Defense Science Board by embarking on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations, a comprehensive set of safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices." NIST stated that "[t]hose safeguarding measures include security and privacy controls to protect the critical and essential operations and assets of organizations and the personal privacy of individuals...[and] [t]he ultimate objective is to make the information systems we depend on more penetration resistant to attacks; limit the damage from attacks when they occur; and make the systems resilient and survivable." NIST explained that "[t]he major changes to the publication include:

- Making the security and privacy controls more outcome-based by changing the structure of the controls;
- Fully integrating the privacy controls into the security control catalog creating a consolidated and unified set of controls for information systems and organizations, while providing summary and mapping tables for privacy-related controls;
- Separating the control selection process from the actual controls, thus allowing the controls to be used by different communities of interest including systems engineers, software developers, enterprise architects; and mission/business owners;
- Promoting integration with different risk management and cybersecurity approaches and lexicons, including the Cybersecurity Framework;
- Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks; and
- Incorporating new, state-of-the-practice controls based on threat intelligence and empirical attack data, including controls to strengthen cybersecurity and privacy governance and accountability.

Publication Schedule

At this time, NIST is not updating our publication dates due to a review cycle being incorporated by the Office of Management and Budget, Office of Information and Regulatory Affairs. We will announce these documents as they are cleared for publication.
The references that are affected by this include the following publications:

- **NIST Special Publication 800-18, Revision 2,** *Guide for Developing System Security Plans*

- **NIST Special Publication 800-53, Revision 5 (Final Public Draft),** *Security and Privacy Controls for Information Systems and Organizations.* **Currently in review at the Office of Management and Budget Office of Information and Regulatory Affairs.**
- **NIST Special Publication 800-53A, Revision 5,** *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**
- **NIST Special Publication 800-53B,** *Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**
- **Federal Information Processing Standard (FIPS) 199, Revision 1,** *Standards for Security Categorization of Federal Information and Information Systems.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**
- **Federal Information Processing Standard (FIPS) 200 Revision 1,** *Minimum Security Requirements for Federal Information and Information Systems.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**
- **NIST Special Publication 800-161, Revision 1,** *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**
- **NIST Special Publication 800-171, Revision 2,** *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**
- **NIST Special Publication 800-171B,** *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets.* **On Hold until review cycle completion of SP 800-53 by Office of Management and Budget, Office of Information and Regulatory Affairs due to dependencies on SP 800-53.**

Questions or comments can be submitted to: sec-cert@nist.gov.

Further Reading

"U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say" – *The New York Times*
"American Cyber Command hamstrung Iran's paramilitary force" – *MIT Technology Review*
"French 'cybercops' dismantle pirate computer network" – *BBC News*
"National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook" – *The Wall Street Journal*
"Undersea cable to China may be nixed on national security grounds" – *Al Jazeera*
"Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns" – *The Washington Post*
"Aggressive Amazon tactic pushes you to consider its own brand before you click 'buy'" – *The Washington Post*
"A New HUD Rule Would Effectively Encourage Discrimination by Algorithm" – *Slate*