Technology Policy Update
6 March 2020
By Michael Kans, Esq.

FISA Reauthorization Pulled

On the day the House Judiciary Committee was to mark up a reauthorization of soon to expire Foreign Intelligence Surveillance Act (FISA) provisions, the bill was pulled from consideration after a key Member indicated she would offer a number of amendments that would limit the scope of government surveillance programs. With these FISA provisions expiring on March 15, lawmakers do not have much time to enact legislation. Moreover, a privacy oversight body issued a long-awaited report on the most controversial of the authorities, finding it rife with problematic, even arguably illegal, conduct that produced little intelligence of value.

The Trump Administration asked that Congress permanently extend these programs instead of reauthorizing them for a period of years as has been the custom since passage of the USA PATRIOT Act in 2001. In an August 2019 letter sent before he stepped down, former Director of National Intelligence Dan Coats asked the Senate and House 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." However, a number of stakeholders have balked at a permanent reauthorization of these programs, especially the call detail records program because the NSA has shut down the program. Nonetheless, the Administration is requesting those authorities in the event there is a need in the future.

The House Judiciary Committee set a February 26 markup of the bill that had been agreed upon with the House Intelligence Committee. The "USA FREEDOM Reauthorization Act of 2020" would end the call detail record (CDR) program the National Security Agency (NSA) has operated after former Intelligence Community contractor Edward Snowden exposed the more expansive bulk telephony metadata collection program. In response to these disclosures, Congress passed the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015" (aka the USA FREEDOM Act of 2015) (P.L. 114-23) that barred bulk collection programs like the NSA's and instituted the more targeted CDR program described in the Committee Report:

> if the government can demonstrate a reasonable, articulable suspicion that a specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation therefor, the Foreign Intelligence Surveillance Court (FISC) may issue an order for the ongoing, daily production of call detail records held by telephone companies. The prospective collection of call detail records is limited to 180 days. The government may require the production of up to two "hops"—i.e., the call detail records associated with the initial seed telephone number and call detail records (CDRs) associated with the CDRs identified in an initial "hop."

The "USA FREEDOM Reauthorization Act of 2020" would end the CDR program prospectively, meaning this authority could still be used retrospectively (i.e. past CDRs and investigations.)

However, as the NSA has shuttered the CDR program, these provisions may amount to a de facto closure of the program. The bill would also require the agencies using FISA to obtain warrants for "tangible things" as opposed to FISA orders if a warrant would be required in a criminal investigation. Moreover, any evidence gathered through FISA electronic surveillance would need to be identified as such. The bill would place a deadline on the time within which the Director of National Intelligence must complete its declassification review and public any significant FISA decisions, orders, or opinions. This would need to happen within six months. The powers of FISA amici curiae would be strengthened to allow them to better fulfill their adversarial role. And, the roving wiretap, "lone wolf" provision, and the business records provisions would be extended until December 1, 2023.

According to media accounts, longtime critic of the FISA system, Representative Zoe Lofgren (D-CA), was dissatisfied with the bill, calling it "so pitiful that it is not even worth pursuing." She added that "[w]e have the opportunity to reform the system…[and] [w]e should take that opportunity." Reportedly, Lofgren was going to offer amendments changing the bill to require that an amici curiae be appointed to oppose every government application under FISA to surveil an American and to change the definition of business records to exclude cell phone location, web browsing data, and search history. Information on the other amendments was not made available. Nonetheless, given the disquiet many Republicans have for the FISA program because of surveillance of some associated with the Trump campaign, it is possible Lofgren's amendments would have been adopted, disrupting the carefully negotiated compromise bill.

Lofgren was one of the bipartisan cosponsors of the "Safeguarding Americans' Private Records Act of 2020" introduced in both chambers in late January. In their press release, the sponsors claimed "[t]he bill includes a host of reforms:

- It would permanently end the flawed phone surveillance program, which secretly scooped up Americans' telephone records for years.
- It would close loopholes and prohibit secret interpretation of the law, like those that led to unconstitutional warrantless surveillance programs.
- It would prohibit warrantless collection of geolocation information by intelligence agencies.
- It would respond to issues raised by the Inspector General's office by ensuring independent attorneys, known as amici, have access to all documents, records and proceedings of Foreign Intelligence Surveillance Court, to provide more oversight and transparency.

Notably, beyond revoking the authority for the NSA to restart the telephone collection program, the bill would also exclude from the definition of "tangible thing" in the Section 215 business records exception: Cell site location information, Global positioning system information, Internet website browsing information, and Internet search history information. The bill also contains language that would limit the use of Section 215 to only counterterrorism and foreign intelligence matters and limit the retention of any such material to three years unless it includes foreign intelligence. Moreover, the bill would increase the justification requirements the government must meet before a nondisclosure requirement (aka gag order) can be placed on a company subject to a Section 215 order. The bill also expands the role and powers of the lawyers (aka amici curiae) assigned to argue against FISA warrants and warrantless surveillance. The government would need to submit a report on the use of its roving wiretap authority, which is incidentally one of the expiring authorities. The bill would also set sunset dates for National Security Letter authorities, another means by which surveillance has been conducted by the U.S. government.

This past week, Attorney General William Barr met with Senate Republicans and made the case for an extension of the expiring FISA authorities with the Trump Administration committing to addressing concerns from the right about the FISA process turned up in the Department of Justice's Office of the Inspector General's report on the FISA surveillance of an advisor to the 2016 Trump campaign, Carter Page. It is expected Senate Majority Leader Mitch McConnell (R-KY) will push for a clean reauthorization as he has in the past during other reauthorizations of different FISA authorities. However, fellow Kentucky Senator, Republican Rand Paul claimed President Donald Trump does not want a clean extension and instead wants the program reformed, which, if accurate, would dovetail with his public statements and tweets about what he sees as abusive investigations into his 2016 presidential campaign.

There are other Republicans who support reforming the FISA program. House Judiciary Committee Ranking Member Doug Collins (R-GA) issued a statement after the "USA FREEDOM Act of 2020" was introduced:

- Democrats are completely ignoring the serious abuse committed against President Trump's campaign in 2016, regardless of the fact that Inspector General Horowitz's report confirmed that our intelligence community committed an unforgivable offense when the FBI abused its power to unlawfully spy on Carter Page. There must be accountability for those who committed these offenses and Mr. Nadler's bill fails to impose any penalty on wrongdoers.
- In order to restore the American people's faith in our premier law enforcement agency, we must reform FISA to ensure our intelligence community and FBI are deterred from ever wielding their significant power to spy on American citizens. Any FISA reform bill that moves forward must protect American citizens—including future presidents and presidential campaigns—from unlawful spying. Democrats' bill fails to accomplish this goal, and in fact, makes it more difficult to conduct legitimate surveillance against terrorist targets. The American people deserve better.

Last week, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) released its "Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act" that noted that in only two instances did the CDR program turn up intelligence that was unique and valuable despite having collected over 434 million CDRs in 2018. Opponents of the program have seized on the PCLOB's review to further argue for closing down the CDR program even though the Board did not find any willful violations of the USA FREEDOM Act, the latter point being likely to be used by proponents of the program.

PCLOB noted that "[i]n 2018, the government obtained a relatively low number of FISA court orders—14—and collected a large number of CDRs—more than 434 million, including an unknown number of duplicates, involving 19 million phone numbers." The Board stated that "USA Freedom Act CDRs were cited in 15 intelligence reports over the program's four-year operation…[and] [o]f the 15 reports citing USA Freedom Act CDRs, FBI received unique information from two of the intelligence reports." PCLOB added that "[b]ased on one report, FBI vetted an individual, but, after vetting, determined that no further action was warranted…[and] [t]he second report provided unique information about a telephone number, previously known to US authorities, which led to the opening of a foreign intelligence investigation."

PCLOB asserted:

- The program experienced a series of compliance incidents and data-integrity problems, which led NSA to issue about a dozen notices to the FISA court since 2016. After repeatedly discovering anomalies in the data it received, NSA suspended the collection of CDRs in early 2019. NSA subsequently deleted all CDRs collected under the USA Freedom Act.
- Some of the compliance incidents were of types that could have arisen in other intelligence or equivalent law enforcement collection authorities. These include incidents involving information inadvertently omitted from a FISA court application, certain NSA officers who had access to data without required training, and a provider's production of data beyond the end date of an order.
- Other incidents raise questions unique to the contours of the USA Freedom Act. Beginning in 2016, NSA identified a series of data-integrity problems related to [redacted] and other data errors. In most of these cases, NSA systems unknowingly relied on inaccurate first-hop data to determine which second-hop requests to issue.
- Additional compliance incidents arose from other data errors, such as overwriting of data fields with incorrect or unrelated data.

PCLOB asserted that "[t]hese problems, taken together, contributed to NSA's decision to delete the USA Freedom Act CDR data in 2018 and again in 2019, and its decision to eventually suspend the program…[and] [b]ased on a review of the facts, the Board determined that the compliance incidents were inadvertent, not willful." PCLOB stated that "NSA took steps to remedy each compliance incident, including notifying appropriate oversight entities, imposing additional limits on data requests, and deleting erroneously obtained data…[and] [i]n response to each compliance incident that raised questions about the scope of permitted collection under the statute, NSA chose to follow a narrower, rather than a more expansive, understanding of its authority under the USA Freedom Act."

Senate Sends 5G Bill That Targets Huawei to White House

Last week, the Senate took up and passed the "Secure and Trusted Communications Networks Act" (H.R. 4998) by voice vote, sending the bill to the White House. This is legislation aimed at Huawei and other Chinese companies deemed security risks that may sell their equipment and services to the U.S. and other countries for building 5G networks. The bill would authorize appropriations of $1 billion to help smaller telecommunications systems remove Huawei equipment and use technology the U.S. government claims is safer and more secure.

According to the Committee Report, H.R. 4998 would:

- require the Federal Communications Commission (FCC or Commission) to develop and maintain a list of communications equipment and services that pose an unacceptable risk to national security and prohibit the use of Federal funds administered by the FCC to purchase, rent, lease, or otherwise obtain such equipment and services.
- establish the Secure and Trusted Communications Reimbursement Program to assist small communications providers with the costs of removing prohibited equipment and services from their networks and replacing prohibited equipment with more secure communications equipment and services.

The Committee explained that "[t]he United States identified individual Chinese telecommunications firms, including Huawei Technologies Co. Ltd (Huawei) and its affiliates, as posing significant threats to U.S. commercial and security interests." The Committee claimed

> Large communications companies with sophisticated network security operations and significant capital generally have avoided installing and using Huawei and other suspect foreign equipment in their networks. Moreover, Federal agencies have actively reached out to large carriers to express concerns when carriers have considered purchasing suspect equipment. In contrast, some smaller carriers with more limited resources and less sophisticated security operations have purchased and installed Huawei, and other suspect foreign equipment, in their networks either because the equipment was less expensive or they were unaware of the security risk, or both.

In a section-by-section, the Committee explained in greater detail the salient portions of the bill:

- Section 2 requires the Federal Communications Commission (FCC) to publish and maintain on its website a list of suspect communications equipment or services that could undermine the security of U.S. networks. In publishing this list, the FCC must rely on either a specific determination made by any executive branch interagency body with appropriate national security expertise, a specific determination made by the Department of Commerce under Executive Order 13873, inclusion in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, or a specific determination by a national security agency.
- Section 3 prohibits the use of Federal subsidies made available through programs administered by the FCC from being used to purchase, rent, lease, or otherwise obtain any covered communications equipment or service, or to maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.
- Section 4 requires the FCC to issue regulations within 270 days to establish the "Secure and Trusted Communications Networks Reimbursement Program" to reimburse communications companies with 2 million or fewer subscribers for the costs associated with removing and replacing covered equipment from networks. Applicants for reimbursement under the Program are required to certify to the Commission, at the time of application, that they have developed a plan for the permanent removal, replacement, and disposal of covered equipment and services from their networks.
- Section 8 requires the Administrator of the National Telecommunications and Information Administration to establish a program to share information regarding supply chain security risks with trusted communications providers and trusted suppliers of communications equipment and services.

Washington State Privacy Bill

The Washington State Senate passed an altered version of the "Washington privacy act" (SB 6281), and the Washington State House has altered that bill further in its committee deliberations. The House's version of SB 6281 is under consideration by the House Rules Committee and may soon come to the House floor. However, if the House passes their bill, the Senate would obviously need to agree on final bill text before the package could be sent to the Governor. And, the 2020 legislative session ends on March 12, so time will be of the essence if legislation will be enacted this year.

As noted, the Washington State Senate passed SB 6281 in mid-February after the Senate Ways and Means Committee altered the bill, and among the notable changes made are:

- Delaying the effective date for colleges and non-profits for three years to July 31, 2024

- The state agencies and tribes were included among those entities exempted from meeting the requirements of the new privacy and data security mandates
- Clarifying that one may exercise her right to data portability without also having to also exercise her right of data access
- The provisions on nondiscrimination are expanded to make clear that controllers may not charge different prices or offer lesser services or products if a person exercises his rights under the bill
- Controllers may not "enroll a consumer in a facial recognition service in connection with a bona fide loyalty, rewards, premium features, discounts, or club card program."
- Tightens one of the exceptions allowing controllers and processors to disregard the requirements of the bill but only if it is "essential for the life of the consumer or another natural person" as opposed to being important to their "vital interests."
- Tightens another such exemption by clarifying that controllers and processors may process data for only internal operations
- Expands the definition of "verification" in the context of the new regulatory scheme for facial recognition

The House's Innovation, Technology & Economic Development Committee marked up SB 6281 late last week, and yesterday the House Appropriations Committee held a hearing and approved the bill. Next, the Washington State House Rules Committee will undertake the next step (i.e. "Rules Review") to see if the committee wants the bill to advance. And, of course, operating in the background is the fact the Washington State legislature adjourns on March 12, giving the House and Senate very little time to agree upon and pass a bill the Governor will sign.

In terms of substance, the House Innovation, Technology & Economic Development Committee changed SB 6281 significantly. Notably, the House's bill would give people a private right of action, would make violations of the new privacy law a violation of Washington's Consumer Protection Act (the state's analogue to the FTC Act) that also provides a separate, well-established private right of action, and makes companies jointly and severally liable meaning, for example, a controller could be liable for the entire penalty based on its processor's violations. Also, the one of the thresholds for when companies and other entities are subject to regulation is lowered to the controlling and processing the personal data of 25,000 people and also derives 25% of its gross revenue from selling personal data as opposed to the Senate's bill which set these thresholds at 50,000 people and 50% respectively.

A data controller's data minimization responsibilities would also be tightened. The House's bill provides that "[a] controller's collection of personal data must be only as reasonably necessary to provide services requested by a consumer, to conduct an activity that a consumer has requested, or to verify requests" made by people. In contrast, the Senate's bill allows controllers to collect personal data in ways that are "adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which such data are processed, as disclosed to the consumer."

The House's bill also clarifies the definition of consumer to make clear that a person buying or selling on behalf of herself and her household is considered a "consumer," meaning the suite of consumer rights established under the bill are applicable in broader circumstances than just a person acting for a family or household rather than just in in an individual capacity.

Additionally, local laws, ordinances, or regulations governing the processing of personal data by

controllers or processors that are adopted prior to the effective date of the bill (i.e. July 31, 2021) are not superseded or preempted, thus possibly setting off a push among Washington state jurisdictions to enact more stringent regimes before the state law goes into effect. Also, any facial recognition laws also not preempted or superseded. The bill also tightens when a data controller or processor may share personal data derived from facial recognition with law enforcement to only in response to a court issued warrant.

Finally, two of the Congressional stakeholders on privacy and data security hail from Washington state, and passage of a state law may limit their latitude on a federal bill they could support. Senator Maria Cantwell (D-WA) and Representative Cathy McMorris Rodgers (R-WA), who are the ranking members of the Senate Commerce and House Energy and Commerce's Consumer Protection and Commerce Subcommittee respectively, are involved in drafting their committee's privacy bills, and a Washington state statute may affect their positions in much the same the "California Consumer Privacy Act" (CCPA) (AB 375) has informed a number of California Members' position on privacy legislation, especially with respect to bills being seen as weaker than the CCPA.

NIST Releases Final Guidance on CUI

The National Institute of Standards and Technology (NIST) has released the final version of NIST Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations, the purpose of which "is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI:

> (1) when the CUI is resident in a nonfederal system and organization;
> (2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and
> (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

It bears note the Department of Defense (DOD) relied significantly upon NIST SP 800-171 in drafting the Cybersecurity Maturity Model Certification (CMMC) framework. The DOD explained that "[t]he [CMMC] model encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI specified in NIST SP 800-171 per DFARS Clause 252.204- 7012."

NIST explained that "[t]he requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components…[and] are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations." NIST stated that "[i]n CUI guidance and the CUI Federal Acquisition Regulation (FAR), the CUI Executive Agent will address determining compliance with security requirements."

However, NIST offered this cautionary note at the beginning of the publication:

> The Federal Information Security Modernization Act [FISMA] of 2014 requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems

> used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. This publication focuses on protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations, and recommends specific security requirements to achieve that objective. It does not change the requirements set forth in [FISMA], nor does it alter the responsibility of federal agencies to comply with the full provisions of the statute, the policies established by OMB, and the supporting security standards and guidelines developed by NIST.

NIST explained that "Revision 2 provides minor editorial changes in Chapters One and Two, and in the Glossary, Acronyms, and References appendices…[and] [t]here are no changes to the basic and derived security requirements in Chapter Three."

Finally, NIST has released two companion documents, one of which the agency is still drafting a final version of: SP 800-171A and SP 800-171B (Draft).

Becerra Letter to Congress on CCPA

California Attorney General Xavier Becerra sent a letter to the chairs and ranking members of the House Energy and Commerce and Senate Commerce, Science, and Transportation Committees, urging them not to preempt state privacy laws like the "California Consumer Privacy Act" (CCPA) (AB 375) and to allow people to have the right to sue to enforce any new federal privacy framework.

In the letter to Chairs Frank Pallone Jr (D-NJ) and Roger Wicker (R-MS) and Ranking Members Greg Walden (R-OR) and Maria Cantwell (D-WA), Becerra stated that "I hope that your work can be informed by our undertaking in California...[and] I am optimistic Congress will be able to craft a proposal that guarantees new privacy rights for consumers, includes a meaningful enforcement regime, and respects the good work undertaken by states across the country, looking to state law as providing a floor for privacy protections, rather than a ceiling." Becerra recommended that the committees "develop a final bill that builds on the rights afforded by CCPA and the additional guidance in our regulations." He argued that "Congress should provide consumers with data privacy protections, including but not limited to:

- The right to access, correct, and delete personal data that has been collected;
- The right to minimize data collection, processing, and retention;
- The right to data portability among services; and
- The right to know what data is collected and processed and for what reasons."

It bears note that almost all the major privacy bills that have been released largely meet these dictates with some differences and nuances. Of course, Becerra has defined these rights so broadly that almost all stakeholders can agree on these principles except perhaps the last one. Therefore, as always, it is in the details that different stakeholders will fight, and what constitutes an appropriate right to access, for example, will differ depending on who is defining this right.

Becerra signaled that he is agnostic on whether the Federal Trade Commission or a new agency enforces a new federal standard. He stated that "I welcome a federal partner with the tools and resources for vigorous enforcement of new consumer rights," but without stating his preference as to which agency should be charged with enforcing the new statute. Becerra seems more focused on the scope of powers available to the agency and stated that "it's critical that Congress extend

enforcement powers broadly." Becerra then advocated for state attorneys general to have "parallel enforcement authority," which is an interesting and ambiguous phrase. It is not clear whether Becerra is calling for Congress to allow state attorneys general to enforce the new federal law as virtually all the privacy bills do, or whether he means the bill should not preempt state laws that charge state attorneys general with vindicating the privacy and consumer rights of their citizens. I would suspect the latter given that most of the bills already provide an enforcement role for states.

Finally, Becerra threw his support behind a private right of action, which is not surprising considering the bill he supported in the California legislature last year that would have broadened the CCPA private right of action. Becerra stated "that consumers [should] also have the opportunity to protect their rights directly through a private right of action." Becerra did not, however, discuss some possible contours for a private right of action or how narrowly or broadly this right would be defined. Again, he seems interested in articulating principles.

At the end of the day, Becerra's letter is likely intended more to position him and the California Attorney General's Office regarding federal privacy legislation and possibly to influence California Members who may otherwise be comfortable with federal preemption of the CCPA and a lack of private right of action, to name two of the issues Becerra touched on.

FCC Fines Telcos

In response to media accounts detailing how the four major cellphone carriers were sharing and selling the location data of Americans, the Federal Communications Commission (FCC) completed its investigations and is proposing fines of $200 million on the four companies for violating data privacy and security standards. However, the FCC was not unanimous, and the two Democratic Commissioners thought the FCC should have investigated matters more fully, and one thought the fine structure was inexplicably lax.

The FCC levied the following penalties of

- $57,265,625 against AT&T Inc.
- $12,240,000 against Sprint Corporation
- $91,630,000 against T-Mobile USA, Inc.
- $48,318,750 against Verizon Communications

In each of the Notices of Apparent Liability, the FCC cited the four companies

> for apparently violating section 222 of the Communications Act and the Commission's regulations governing the privacy of customer information. We find that [each named company] apparently disclosed its customers' location information, without their consent, to third parties who were not authorized to receive it. In addition, even after highly publicized incidents put the [each named company] on notice that its safeguards for protecting customer location information were inadequate, [each named company] apparently continued to sell access to its customers' location information for the better part of a year without putting in place reasonable safeguards—leaving its customers' data at unreasonable risk of unauthorized disclosure.

The FCC explained

> The Act and the Commission's rules govern and limit telecommunications carriers' use and disclosure of certain customer information. Section 222(a) of the Act imposes a general duty on telecommunications carriers to "protect the confidentiality of proprietary information" of "customers." Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI, namely information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship." The Commission has issued regulations implementing the privacy requirements of section 222 (CPNI Rules), and has amended those rules over time. Most relevant to this proceeding are the rules that the Commission adopted governing customer consent to the use, sharing, or disclosure of CPNI and those relating to carriers' duty to discover and protect against unauthorized access to CPNI.

Chair Ajit Pai explained the action:

> we also make clear that we will not hesitate to vigorously enforce these statutory provisions and regulations. After a thorough investigation, we find that all of our nation's major wireless carriers apparently failed to comply with these vitally important requirements. In brief, long after these companies were on notice that their customers' location data had been breached, they continued to sell access to that data for many months without taking reasonable measures to protect it from unauthorized disclosure. This FCC will not tolerate any telecommunications carrier putting American consumers' privacy at risk. We therefore propose fines against these four carriers totaling more than $200 million.

Commissioner Jessica Rosenworcel stated in her dissent:

- in the end I find this enforcement action inadequate. There are more than 270 million smartphones in service in the United States and this practice put everyone using them at a safety risk. The FCC heavily discounts the fines the carriers could owe under the law and disregards the scope of the problem.
- Here's why. At the outset, the FCC states that this impermissible practice should be the subject of a fine for every day that it was ongoing. But right at the outset the agency gives each carrier a thirty-day pass from this calculation. This thirty day "get-out-of-jail-free" card is plucked from thin air. You'll find it in no FCC enforcement precedent. And if you compare it to every data security law in the country, this stands as an outlier. In fact, state privacy laws generally require companies to act on discovered breaches on a much faster timetable—in some cases, less than a week. Real-time location data is some of the most sensitive information available about all of us and it deserves the highest level of privacy protection. Permitting companies to turn a blind eye for thirty days after discovering this data is at risk falls short of any reasonable standard.
- Next, the FCC engages in some seriously bureaucratic math to discount the violations of our privacy laws. The agency proposes a $40,000 fine for the violation of our rules—but only on the first day. For every day after that, it imposes only a $2,500 fine for the same violation. But it offers no acceptable justification for reducing the fine in this way. Plus, given the facts here—the sheer volume of those who could have had their privacy violated—I don't think this discount is warranted.

House Energy & Commerce Committee Chair Frank Pallone Jr. (D-NJ) issued a statement:

> Today's notice by the FCC confirms what I have said from the beginning — carriers have a duty to protect consumers' real-time location data and the FCC must enforce the law in order to protect the personal safety of consumers across the country. While I am glad the FCC is finally proposing fines for this egregious behavior, it represents little more than the cost of doing business for these carriers. Further, the Commission is still a long way from collecting these fines and holding the companies fully accountable.

In January 2019, key Democrats urged the FCC to investigate the claims in the *Motherboard* article that alleged "T-Mobile, Sprint, and AT&T are selling access to their customers' location data." Pallone sent a letter to the FCC asking for a briefing to explain why the FCC "has yet to end wireless carriers' unauthorized disclosure of consumers' real-time location data and what actions the FCC has taken to address this issue to date." Pallone asserted that these issues were addressed in the rewrite of telecommunications law in 1996, but that the FCC has "dragged its feet in protecting consumers." In his press release, Pallone summarized the recent history of allegations of service providers sharing location information:

> Last May, investigative journalists and U.S. Senator Ron Wyden (D-OR) helped bring to light the ease with which consumers' real-time location data was being made available to the public without the users consent. Following those revelations, the FCC referred the allegations to its Enforcement Bureau for investigation. In June, some wireless carriers publicly committed to addressing the issue and put an end to this unauthorized disclosure. Yet a new report this week indicates this unfortunate practice continues.

Senator Ron Wyden (D-OR) contended in statement:

> Based on today's news reports, it seems clear Chairman Pai has failed to protect American consumers at every stage of the game – this issue only came to light after my office and dedicated journalists discovered how wireless companies shared Americans' locations willy nilly. He only investigated after public pressure mounted. And now his response is a set of comically inadequate fines that won't stop phone companies from abusing Americans' privacy the next time they can make a quick buck.

In January 2019, Wyden and 14 other Senate Democrats asked "the Federal Trade Commission and FCC to investigate how wireless carriers allowed third parties – including data brokers and bounty hunters – to track Americans' cell phones without consent."

EU Cyber Risk Report

The European Systemic Risk Board (ESRB) released a report titled, "Systemic cyber risk," that examined hypothetical scenarios under which cyber incidents could pose systemic risks to Europe's and the world's financial systems. The ERSB explained that

> Cyber risk is characterised by three key features that, when combined, fundamentally differentiate it from other sources of operational risk: the speed and scale of its propagation as well as the potential intent of threat actors. The interconnectedness of various information systems enables cyber incidents to spread quickly and widely. Some recent incidents have

> demonstrated actors' ability to penetrate the networks of large organisations and incapacitate them quickly. Cyber incidents can also spread widely across sectors and beyond geographical borders, including to entities which are not the primary target or source of disruption. Malicious cyber incidents are becoming more persistent and prevalent, illustrating the high level of sophistication and coordination that threat actors are able to achieve.

The ERSB asserted that it "has developed an analytical framework to assess how cyber risk can become a source of systemic risk to the financial system." The ERSB stated that

> The four stages of this conceptual model (context, shock, amplification, systemic event) facilitate a systematic analysis of how a cyber incident can grow from operational disruption into a systemic crisis. In particular, the framework could assist in analysing systemic vulnerabilities that amplify the shock of a cyber incident, and in understanding at which point a cyber incident may become systemic. The ESRB also surveyed its membership to form a view on common individual vulnerabilities across ESRB jurisdictions. Combining these elements, the ESRB has considered a number of historical and hypothetical scenarios. It used these scenarios to try to understand the distinction between severe operational disruption to the financial system, on the one hand, and a systemic crisis, on the other hand.

The ERSB stated that

> A cyber incident can evolve into a systemic crisis when trust in the financial system is eroded. A critical point in assessing whether a cyber incident will progress to become a systemic financial crisis lies in the differentiation of whether or not the incident escalates from an operational level into the financial and confidence realms. In order for a cyber incident to raise systemic financial and confidence concerns, either the disruption to critical functions supporting the real economy or the generated (or anticipated) financial losses from the incident need to reach a level where the financial system is no longer able to absorb the shock. For instance, a perceived irrecoverable destruction, alteration or encryption of account balances of one or several financial institutions could constitute a sufficiently severe shock to the financial system. This could occur through operational disruption, financial losses and loss of confidence in the system, triggering liquidity freezes, bank runs and panic. The loss of confidence in the integrity of data could in itself trigger similar reactions.

The ERSB asserted that

> To mitigate further the risk of a systemic cyber incident materialising, more work is required to address system vulnerabilities and reduce the potential for widespread disruption through amplification channels. The scenario analysis in this report reveals that the loss of confidence in the financial system plays a key role in a cyber incident developing into a systemic crisis. A number of policy areas therefore merit further exploration:
>
> - First, given the speed and scale at which such a cyber incident may unfold, rapid coordination between stakeholders and a consistent and clear communication from authorities may be required in order to shore up confidence. Different ongoing work streams could be leveraged to achieve this goal.
> - Second, effective restoration of key economic functions requires planning, including agreeing on a clear division of tasks between industry and authorities, and between (technical) incident management and (financial) consequence management. This may also

include reflections on central bank emergency communications, interventions or assistance when a cyber crisis becomes a financial stability crisis.

- Finally, the cyber equivalent of capital buffers is preparedness and resilience. In that sense, the operationalisation of systemic resilience mechanisms such as data vaulting, among other things, merits further exploration. This is of particular importance as many recovery and resolution plans are contingent on essential data being available or recoverable.

The ESRB stated that it "intends to explore some of the potential systemic mitigants in future work…[and] [t]aking stock of the findings in this report, the ESRB intends to leverage its broad institutional composition and network to evaluate the costs and benefits of different systemic mitigants going forward."

The ERSB contended that "[t]he analytical framework suggests that a truly systemic event would require a severe shock, an alignment of amplifiers and a lack of effective systemic mitigants…[and] [a]s argued throughout the report, the financial system displays a number of vulnerabilities, which together create a context in which a systemic cyber crisis could unfold." The ERSB stated that "[i]n all of the hypothetical scenarios presented in Section 3, the greatest damage to the financial system occurred when multiple amplifiers were activated and what was initially an operational crisis triggered a sufficiently severe loss of confidence in financial institutions and markets." The ERSB added that "the hypothetical scenarios indicated that financial market participants on their own would not be able to resolve the crisis, but instead required support from financial and non-financial authorities."

The ERSB stated that "[a]dditional efforts are required to reduce the potential impact of such a crisis and the likelihood of it happening." The ERSB said that "[a]s indicated in Section 2, both public authorities as well as private entities are undertaking a significant number of initiatives to reduce cyber-related risks." The ERSB asserted that "[w]hile the characteristics of cyber risk make it extremely difficult (or costly) to fully eliminate it, there are a number of policy areas that deserve more exploration to identify and mitigate systemic cyber vulnerabilities, thus further reducing systemic cyber risk." The ERSB stated that "[i]n some instances macroprudential tools may be appropriate, while in others (traditional) central bank intervention may be required…[and] [m]icroprudential supervision, an improved level of cyber hygiene and a collective industry response are additional key building blocks."

AI Update Released

The White House's Office of Science and Technology Policy (OSTP) has released the "American Artificial Intelligence Initiative: Year One Annual Report" in which the agency claimed "the Trump Administration has made critical progress in carrying out this national strategy and continues to make United States leadership in [artificial intelligence] (AI) a top priority." Last February, the Administration started the American Artificial Intelligence Initiative, "the Nation's strategy for promoting American leadership in AI" with the issuance of Executive Order (EO)13859 and various follow on actions have flowed directly from directives in the EO. OSTP asserted that "[s]ince the signing of the EO, the United States has made significant progress on achieving the objectives of this national strategy...[and] [t]his document provides both a summary of progress and a continued long-term vision for the American AI Initiative." However, some agencies were working on AI-related

initiatives independently of the EO, but the White House has folded those into the larger AI strategy it is pursuing. Much of the document recites already announced developments and steps.

However, OSTP seems to reference a national AI strategy that differs a bit from the one laid out in EO 13859 and appears to represent the Administration's evolved thinking on how to address AI across a number of dimensions in the form of "key policies and practices:"

1) ***Invest in AI research and development:*** The United States must promote Federal investment in AI R&D in collaboration with industry, academia, international partners and allies, and other non- Federal entities to generate technological breakthroughs in AI. President Trump called for a 2-year doubling of non-defense AI R&D in his fiscal year (FY) 2021 budget proposal, and in 2019 the Administration updated its AI R&D strategic plan, developed the first progress report describing the impact of Federal R&D investments, and published the first-ever reporting of government-wide non-defense AI R&D spending.

2) ***Unleash AI resources****:* The United States must enhance access to high-quality Federal data, models, and computing resources to increase their value for AI R&D, while maintaining and extending safety, security, privacy, and confidentiality protections. The American AI Initiative called on Federal agencies to identify new opportunities to increase access to and use of Federal data and models. In 2019, the White House Office of Management and Budget established the Federal Data Strategy as a framework for operational principles and best practices around how Federal agencies use and manage data.

3) ***Remove barriers to AI innovation****:* The United States must reduce barriers to the safe development, testing, deployment, and adoption of AI technologies by providing guidance for the governance of AI consistent with our Nation's values and by driving the development of appropriate AI technical standards. As part of the American AI Initiative, The White House published for comment the proposed United States AI Regulatory Principles, the first AI regulatory policy that advances innovation underpinned by American values and good regulatory practices. In addition, the National Institute of Standards and Technology (NIST) issued the first-ever strategy for Federal engagement in the development of AI technical standards.

4) ***Train an AI-ready workforce****:* The United States must empower current and future generations of American workers through apprenticeships; skills programs; and education in science, technology, engineering, and mathematics (STEM), with an emphasis on computer science, to ensure that American workers, including Federal workers, are capable of taking full advantage of the opportunities of AI. President Trump directed all Federal agencies to prioritize AI-related apprenticeship and job training programs and opportunities. In addition to its R&D focus, the National Science Foundation's new National AI Research Institutes program will also contribute to workforce development, particularly of AI researchers.

5) ***Promote an international environment supportive of American AI innovation****:* The United States must engage internationally to promote a global environment that supports American AI research and innovation and opens markets for American AI industries while also protecting our technological advantage in AI. Last year, the United States led historic efforts at the Organisation for Economic Cooperation and Development (OECD) to develop the first international consensus agreements on fundamental principles for the stewardship of trustworthy AI. The United States also worked with its international partners in the G7 and G20 to adopt similar AI principles.

6) ***Embrace trustworthy AI for government services and missions****:* The United States must embrace technology such as artificial intelligence to improve the provision and efficiency of

government services to the American people and ensure its application shows due respect for our Nation's values, including privacy, civil rights, and civil liberties. The General Services Administration established an AI Center of Excellence to enable Federal agencies to determine best practices for incorporating AI into their organizations.

Among the federal government's AI efforts that OSTP chose to highlight are:

- Collaboration across the Federal Government can also be fostered through a Center of Excellence (COE) model, which can serve as an important mechanism for agencies to share AI expertise and best practices. The General Services Administration (GSA) has launched an AI COE to enable agencies to develop AI solutions by incorporating machine learning, computer vision, natural language processing, intelligent process design, and robotic process automation into their operations.
- In other efforts, [the Department of Defense] (DOD) established the Joint Artificial Intelligence Center (JAIC) to serve as the focal point for the execution of the DOD AI Strategy and as an AI Center of Excellence. The JAIC aims to accelerate DOD's adoption of AI through repeatability at scale, creating leveraged products, policies, people, platforms, and processes. Its products focus on a set of challenging use cases that can benefit from AI, including Joint Warfighting Operations; Warfighter Health; Predictive Maintenance; Intelligent Business Automation; Humanitarian Assistance and Disaster Relief; and Cyber Sensemaking.
- [The Department of Energy] (DOE) established the Artificial Intelligence and Technology Office (AITO) to serve as a nexus for coordinating AI activities and accelerating intradepartmental and interagency collaborations. AITO is working on projects with the VA, Health and Human Services, and the JAIC to create AI solutions that address our Nation's health priorities and will enable humanitarian assistance and disaster response for wildfires and floods.
- Federal agencies have also been very active over the past year in implementing their own strategies and actions to advance their missions using AI. Several agencies have released their own AI and data science strategies, including the NIH Strategic Plan for Data Science, the DOD AI Strategy, and the National Oceanic and Atmospheric Administration (NOAA) AI Strategy.
- Agencies are also setting up centers and offices focused on coordinating and advancing AI activities across their agency, such as DOD's JAIC, DOE's AITO, and the VA's National AI Institute.
- The United States Patent and Trademark Office is engaging with the innovation community and experts in AI to consider potential guidance on patenting AI inventions, issuing a request for comments to gather information from interested stakeholders.
- DOT has released a series of guidance reports for how best to integrate automated vehicles into our transportation system.

EDPB Statement on Google's Proposed Acquisition of Fitbit

The European Data Protection Board (EDPB) made clear it position that Google and Fitbit will need to scrupulously observe the General Data Protection Regulation's privacy and data security requirements if the body is sign off on the proposed $2.2 billion acquisition. Moreover, at present Google has not informed European Union (EU) regulators of the proposed deal. The deal comes at a time when both EU and U.S. regulators are already investigating Google for alleged antitrust and anticompetitive practices, and the EDPB's opinion could carry weight in this process.

The EDPB stated "[t]here are concerns that the possible further combination and accumulation of sensitive personal data regarding people in Europe by a major tech company could entail a high level of risk to the fundamental rights to privacy and to the protection of personal data." The EDPB added:

- The EDPB has previously stated that it is essential to assess longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed. The EDPB therefore reminds the parties to the proposed merger, in accordance with the principle of accountability, of their obligations under the GDPR and to conduct in a transparent way a full assessment of the data protection requirements and privacy implications of the merger.
- The EDPB urges the parties to mitigate the possible risks of the merger to the rights to privacy and data protection before notifying the merger to the European Commission. The EDPB will consider the implications that this merger may have for the protection of personal data in the European Economic Area and stands ready to contribute its advice on the proposed merger to the Commission if so requested. The EDPB will continue to be vigilant in this and similar cases in the future.

In late November 2019, the European Commission (EC) confirmed in an email to Reuters that it is investigating Google's data practices. The EC stated "[t]he Commission has sent out questionnaires as part of a preliminary investigation into Google's practices relating to Google's collection and use of data…[and] [t]he preliminary investigation is ongoing." Reuters claimed "the EU's focus is on data related to local search services, online advertising, online ad targeting services, login services, web browsers and others."

This is not Google's first brush with EU antitrust regulators. In March 2019, European regulators fined Google €1.49 billion for abusive practices in online advertising. In May 2018, the EU levied a €4.34 billion fine "for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine."

And, Google is currently being investigated by the U.S. Department of Justice for possible antitrust violations as part of the government's broader look into how big technology companies operate. The Federal Trade Commission also recently announced it had requested 10 years of materials from Google among four other companies on the merger and acquisition activities that fall below the threshold that automatically triggers scrutiny from the federal government.

DOD Adopts AI Ethics

The Department of Defense (DOD) announced in a press release that it "officially adopted a series of ethical principles for the use of Artificial Intelligence today following recommendations provided to Secretary of Defense Dr. Mark T. Esper by the Defense Innovation Board last October." The DOD claimed "[t]he adoption of AI ethical principles aligns with the DOD AI strategy objective directing the U.S. military lead in AI ethics and the lawful use of AI systems." The Pentagon added "[t]he DOD's AI ethical principles will build on the U.S. military's existing ethics framework based on the U.S. Constitution, Title 10 of the U.S. Code, Law of War, existing international treaties and longstanding norms and values." The DOD stated "[t]he DOD Joint Artificial Intelligence Center (JAIC) will be the focal point for coordinating implementation of AI ethical principles for the department."

The DOD explained that "[t]hese principles will apply to both combat and non-combat functions and assist the U.S. military in upholding legal, ethical and policy commitments in the field of AI...[and] encompass five major areas:

- Responsible. DOD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.
- Equitable. The Department will take deliberate steps to minimize unintended bias in AI capabilities.
- Traceable. The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.
- Reliable. The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.
- Governable. The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

It bears note that the DOD's recitation of these five AI Ethics differs from those drafted by the Defense Innovation Board. Notably, in "Equitable," the Defense Innovation Board also included that the "DOD should take deliberate steps to avoid unintended bias *in the development and deployment of combat or non-combat AI systems that would inadvertently cause harm to persons*" (emphasis added.) Likewise, in "Governable," the Board recommended that "DOD AI systems should be designed and engineered to fulfill their intended function while possessing the ability to detect and avoid *unintended harm or disruption, and for human or automated disengagement or deactivation of deployed systems that demonstrate unintended escalatory or other behavior* (emphasis added.)

Additionally, the DOD has declined, at least at this time, to adopt the recommendations made by the Board regarding the use of AI:

1. Formalize these principles via official DOD channels.
2. Establish a DOD-wide AI Steering Committee.
3. Cultivate and grow the field of AI engineering.
4. Enhance DOD training and workforce programs.
5. Invest in research on novel security aspects of AI.
6. Invest in research to bolster reproducibility.
7. Define reliability benchmarks.
8. Strengthen AI test and evaluation techniques.
9. Develop a risk management methodology.
10. Ensure proper implementation of AI ethics principles.
11. Expand research into understanding how to implement AI ethics principles.
12. Convene an annual conference on AI safety, security, and robustness.

Of course, the DOD's adoption of AI Ethics came amidst a backdrop of increasing Administration and international interest in proper regulation of these new technologies. Last month, the Office of Management and Budget (OMB) requested comments on a draft "Guidance for Regulation of Artificial Intelligence Applications" that would be issued to federal agencies as directed by Executive Order (EO) 13859, "Maintaining American Leadership in Artificial Intelligence" that "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." OMB listed the 10 AI principles agencies must in regulating AI in the private sector, some of which have some overlap with the DOD's Ethics:

- 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

Finally, the European Commission (EC) recently released its latest policy pronouncement on artificial intelligence, "On Artificial Intelligence - A European approach to excellence and trust," in which the Commission articulates its support for "a regulatory and investment oriented approach with the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of this new technology." The EC stated that "[t]he purpose of this White Paper is to set out policy options on how to achieve these objectives...[but] does not address the development and use of AI for military purposes." The EC is accepting comments until May 19, 2020, most of which will be made public.

Further Reading

- "The Pentagon Is Sitting on a Chunk of Valuable Airwaves. Why?" – *Politico*. This comprehensive primer on U.S. spectrum issues points to a major stumbling block in trying to beat China in the 5G race: the Department of Defense currently controls the valuable mid-band spectrum that experts and private sector stakeholders argue is best suited for next generation communications. Worse still, China and the rest of the world are moving forward into these mid-band frequencies, meaning that unless the Pentagon develops alternatives, its ability to operate in other parts of the world may be compromised by having to share these spectrums. Finally, the Trump Administration does not have a coherent approach even as the DOD is trying to reach agreement with private sector companies like telecommunications companies.
- "Digital Edits, a Paid Army: Bloomberg Is 'Destroying Norms' on Social Media" – *The New York Times*. Mike Bloomberg's campaign pushed the limits of what social media platforms allow influencers and users to say about political matters without explicitly revealing their allegiance to or payment from a presidential campaign. Bloomberg has poured millions into recruiting and activating social media users to advocate for his campaign, far outpacing rivals for the Democratic nomination and possibly suggesting a playbook for the eventual Democratic nomination. Facebook, Twitter, and Instagram struggled to keep up with a number of the Bloomberg campaigns moves.
- "Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen" – *Daily Beast*. "Clearview AI's Massive Client List Got Hacked" – *WIRED*; "The world's scariest facial recognition company is now linked to everybody from ICE to Macy's" – *Recode*; "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE,

Macy's, Walmart, And The NBA" – *BuzzFeed*; and "Clearview AI Reports Breach of Customer List" – *Motherboard*. The company that has scraped the images of people from multiple websites for use with artificial intelligence facial recognition technology has gotten much more recognition lately, most of it scrutiny the company would just as likely want to avoid. After a breach of its client list (including a number of law enforcement agencies), numerous entities denied being client, claimed they only tried the service, or asserted they would never use the service. These reports come amidst statements by multiple governments they will investigate the company's practices. Among the law enforcement agencies that are likely using Clearview AI are: U.S. Immigration and Customs Enforcement (ICE), the US Attorney's Office for the Southern District of New York, the Federal Bureau of Investigation (FBI)I, Customs and Border Protection (CBP), Interpol, and many local police departments.

- "Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders" – *The Markup*. One insurer tried to convince a state regulator to increase supposedly outdated car insurance premiums and was required to submit voluminous additional information. Maryland ultimately turned down Allstate, in large part because the analysis of the underlying algorithm showed it was designed to inflict the largest increases on those willing to pay much more. This is not the first instance of differential pricing and with algorithms and big data, more is almost certainly on the way.
- "Europe's bid to stay world's digital cop fizzles to life" – *Politico*. This piece questions how much impact the European Union (EU) will have in trying to compete with the U.S. and China in shaping the future of technology and accompanying policy.
- "Justice Department faults Google for turning over evidence too slowly in antitrust probe, hinting at possible legal action" – *The Washington Post*. The Department of Justice sent a letter to Google possibly threatening legal process to get documents the company is producing too slowly or not at all. This document request will likely inform the agency's larger antitrust investigation into big technology companies.