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

Spotlight: A Privacy Bill A Week

Key Points:

- *This bill is far more comprehensive and consumer-friendly than virtually all other bills, and so is unlikely to be enacted given Republican control of the Senate and the number of moderate Democrats in the House*
- *Instead of serving as a vehicle of what's possible, this bill is a marker for privacy and civil liberties advocates and is designed to pull Democrats to the left in crafting a House bill and during negotiations on a final bill*
- *This bill eschews an enhanced notice and consent regime and rules out certain practices, gives the FTC a sweeping mandate to draft regulations, allows consumers to sue, does not preempt state laws, and mandates data security along with requiring privacy protection*

Last week, we delved into the "Social Media Privacy Protection and Consumer Rights Act of 2019" (S. 189), but this week we will look at a bill that probably exceeds bounds of the politically possible: the "Privacy Bill of Rights Act" (S. 1214), the only bill to get an A in the Electronic Privacy Information Center's report on privacy bills. The definition of "personal information" is easily the most expansive of any of the bills we've looked at and would impose more and various new duties on covered entities than any of the bills we've analyzed.

This bill goes beyond an enhanced notice and consent regime and would declare some current data practices as illegal subject to Federal Trade Commission (FTC) enforcement. To wit, the bill provides "[i]t shall be unlawful for any covered entity to commit an act prohibited under this Act or a regulation promulgated under this Act, regardless of any specific agreement between entities or individuals." There is also an interesting provision regarding unexpected data collection and usage that may have been crafted to foil those looking to exploit loopholes.

The bill defines "covered entities" so broadly that virtually any person or entity collecting the data of people in the U.S. would be included. To wit, the bill defines a "covered entity" as "any person that collects or otherwise obtains personal information." Note that this definition is not limited to online entities; rather, anyone collecting and sharing information would be subject, making this bill among the most sweeping of those we have analyzed.

With respect to responsibilities under the "Privacy Bill of Rights," covered entities must protect the privacy of personal information in their care and also ensure that this information is safe from unauthorized access. These entities must also obtain the affirmative, express, knowing consent of consumers before they can collect, use, retain, share, or sell this information through the provision of notice.

In terms of who would be covered by the protections in the bill, it would be virtually everyone in the U.S. and possibly people overseas as well. The bill is not clear on this, presumably in order to provide the broadest amount of data rights to the widest group of individuals possible. However, minors are defined as those being 16 years of age and under. The bill provides that "[t]o the extent

that a provision of this Act or a regulation promulgated under this Act is inconsistent with a provision of any other Federal law relating to the protection and control of the personal information of minors, the provision that provides the most protection and control to minors and their parents or guardians shall apply."

The "Privacy Bill of Rights" contains one of the broadest, most sweeping definitions of the type of data that shall be protected. The bill provides "personal information…means information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to, a particular individual." Moreover, thereafter follows a lengthy and exhaustive list of examples of data that qualifies as "personal information," which is too long to reasonably quote. But, of all the bills we have looked at thus far, this is the most comprehensive definition, and because this list is presented as "examples," it may follow that the regulations to be promulgated could include other personal information that is to be protected and secured.

There are incentives in the bill to de-identify data, and what shall be deemed de-identified "is "information that cannot reasonably identify, relate to, describe, or be capable of being associated with or linked to, directly or indirectly, a particular individual." In terms of the policy backdrop, this incentive structure seems designed to drive covered entities to make data less valuable over time to hackers but also prevent future uses contrary to the original purpose of the data collection.

However, the FTC is empowered to grant specific exemptions to the requirement that consumers must affirmatively and knowingly opt-in to the collection and use of their personal information on the basis of any privacy risks posed by how the covered entity is using the data, the costs and benefits of applying these requirements, and the extent to which the personal information is necessary to and used for the security of the covered entity, consistent with the service of product provided, and de-identified, among other considerations. Any exempted entities must be listed on the FTC's website along with a "brief justification" as to why the entity was exempted.

The FTC would be empowered to police a vast range of practices of covered entities related to the collection and use of personal information. However, a few definitions worth mentioning regarding this part of the "Privacy Bill of Rights."

A "breach of security" is "any instance in which a person, without authorization or in violation of any authorization provided to the person, gains access to, uses, or discloses personal information." This definition covers the expected situation of a hacker somewhere getting into a system or information he has no authorization to access. However, it also covers situations where a person is accessing information "in violation of the authorization" granted to a person or organization. Consequently, if an organization that has authorization to hold and use my personal information on my baseball card collection but not to share subsequently sends this information to a data broker, this would be a breach of security.

Additionally, the "Privacy Bill of Rights" defines the word "disclose" in sweeping fashion, meaning "to disclose, release, transfer, share, disseminate, make available, or otherwise communicate orally, in writing, electronically, or by any other means to any third party." It is hard to conceive of a means to share or transmit information to a third party not covered by this definition.

Covered entities must obtain opt-in approval from a person before any collection or sharing of that person's data may happen. The bill defines opt-in approval as "affirmative, express consent of an individual for a covered entity to use, disclose, or permit access to the individual's personal

information after the individual has received explicit notification of the request of the covered entity with respect to that information." The FTC will promulgate regulations to "require a covered entity to obtain opt-in approval from an individual to—

(1) collect, use, retain, share, or sell the individual's personal information; or

(2) make any material changes in the collection, use, retention, sharing, or sale of the individual's personal information."

Additionally, "[a]n individual shall have the right to withdraw his or her approval at any time." However, under specified "emergency or exigent circumstances," a covered entity would not need opt-in approval to collect, use or share personal information, and these include where "the covered entity, in good faith, believes danger of death or serious physical injury to any individual requires use, access, or disclosure without delay of personal information relating to the emergency."

The bill lays out a very robust list of information consumers must be given notice of "a short-form notice about the collection, retention, use, and sharing of the personal information of individuals by the covered entity" that includes:

- What personal information is being collected, used, or retained
- How this personal information is collected, and how, and for what purpose, it is being sold, shared, used, retained, or collected
- Third parties with whom the information is sold, shared, or leased and for what purpose
- How a person can access, correct, delete, or request the personal information held by the covered entity
- Any offline practices for collecting information not related to the online behavior of a person; and
- The right of a person to opt-in or withdraw approval for the collection and use of personal information.

Any such notice will need to be concise, complete, intelligible, and well-written. Additionally, covered entities will need to update their notice within 15 days of making a "material" change to their privacy policy or practices. Additionally, covered entities must post notice in a clear and conspicuous place on their website and keep this notice posted. Also, this notice must be furnished to a consumer before she buys a product, service, or subscription, or establishes an account.

The FTC will also promulgate regulations to govern the "unexpected" collection or use of personal information. In these situations, covered entities must provide the same notice as under normal circumstances, including the option to opt-in and would also have a responsibility to inform the consumer of any material changes in the same way as for normal collection and use practices. Covered entities would be barred from collecting any personal information not listed in the notice and must provide new notice each time the universe of data they collect changes. Likewise, the same applies to the purposes for which personal information is used. Covered entities would be excused from these requirements if the collection and use of personal information

- "is necessary for the performance of a contract to which the individual is party;
- consists of actions that an individual would consider necessary in order to provide a requested product or service; or
- consists of actions taken at the request of the individual prior to entering into a contract to which the individual is party."

Covered entities must allow consumers a reasonable opportunity and process to access, correct, delete, and obtain their personal information. Moreover, covered entities would have a duty to

provide a description of the information being held, when the collection of information began, for how long the information will be retained, and the third parties with whom the information has been shared. There are a number of exceptions to the requirement that a covered entity delete personal data upon request, including:

- If the personal information is needed to secure the covered entity's system
- To exercise the free speech rights of the consumer or another person
- To comply with federal statutes on electronic communications surveillance

Covered entities must also "inform any entity with which the covered entity has shared, sold, or disclosed an individual's personal information of any request from the individual for confirmation of, access to, correction of, or deletion of the individual's personal information." Likewise, a covered entity would need to comply with a consumer's request if it is conveyed by another covered entity. Additionally, "[a] covered entity may not de-identify an individual's personal information during the 90-day period beginning on the date on which the covered entity receives a request from the individual for confirmation, access, correction, or deletion of the individual's personal information." The FTC is also charged with promulgating regulations for these processes.

Covered entities must "ensure that personal information that has been de-identified is not restored such that the information can be linked to a specific individual or device," and the FTC's regulations would include this duty.

Covered entities may neither pose consumers with take-it-or-leave-it offers nor may they offer financial incentives for consumers to opt-in to data collection and use. Unlike some of the other bills we have analyzed, the Privacy Bill of Rights forbids covered entities from denying service to consumers who do not opt-in to "the collection, use, retention, sharing, or sale of the individual's personal information for commercial purposes" (aka a "take-it-or-leave-it-offer"). In the same vein, covered entities cannot offer people a discount or incentive to get them to opt-in. However, the FTC may determine that certain types of financial incentives are permissible if they "reasonable, just, and non-coercive." One wonders what type of financial incentives would be greenlighted under an FTC that seeks to take a "light regulatory touch," and there does not seem to be a means by which the FTC would be empowered to rescind such a determination.

S. 1214 would tightly circumscribe how an individual's personal information may be disclosed by a covered entity to a third-party under a written contract. However, there are exceptions for covered entities sharing with third parties in response to a legal process such as a warrant or subpoena or in order to protect a person's property or to address security or technical issues.

Section 11 of the bill details the practices that would be illegal under the "Privacy Bill of Rights." Notably, covered entities would be prohibited from "selling, leasing, trading, or otherwise profiting from an individual's biometric information." If a covered entity obtains "specific consent" from a person, it may share, reshare, or otherwise disseminate an individual's biometric information; however, specific consent would not be required if dissemination "is required by State or Federal law or municipal ordinance; or…is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction."

Likewise, S. 1214 outright bans a number of current practices that have been deemed "digital redlining" and others:

- processing personal information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for

employment, finance, healthcare, credit, insurance, housing, or education opportunities, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person's or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability; or

- processing personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person's or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, or disability.

There are additional prohibitions on what covered entities may do with the personal information it collects. Section 12 bars collection data "beyond what is adequate, relevant, and necessary—

for the performance of a contract to which the individual is party;
to provide a requested product or service; or
to take steps at the request of the individual prior to entering into a contract to which the individual is party."

Additionally, there would be limits on how long after a covered entity has finished using the information that it may access the information. Notably, 90 days after the latest of any of these dates, a covered entity would not able to access the information:

- the covered entity concludes the performance of a contract to which the individual is party;
- the covered entity concludes taking steps that an individual would consider necessary in order to provide a requested product or service, including steps to prevent fraud, ensure safety, or ensure compliance with the covered entity's terms of service; or
- the individual otherwise terminates his or her relationship with the covered entity."

Unlike a number of other bills, the "Privacy Bill of Rights," the FTC would be required to promulgate data security regulations. Some Democratic stakeholders such as Senate Commerce, Science, and Transportation Committee Ranking Member Maria Cantwell (D-WA) would like any privacy bill to be paired data security legislation, for, in her view, the two issues are inseparably intertwined. The FTC would draft regulations "require a covered entity to establish and maintain reasonable data security practices to protect the confidentiality, integrity, and availability of personal information…that are proportional to the volume and nature of the personal information a covered entity collects." This approach is not entirely alien with how the FTC currently approaches data security cases under its Section 5 powers to prohibit unfair and deceptive practices. Covered entities would be required to alert people in the event of a security breach if

- an unauthorized disclosure of the personal information of the individual has occurred; and
- harm is reasonably likely to occur

The FTC will likely wrestle with determining what constitutes when "harm is reasonably likely to occur," and with what constitutes harm. Industry and many Republicans will probably argue that harm should be defined to be actual, concrete economic harm such as identity theft. This will matter, for if a security incident is defined so tightly as to be only cases of economic harm, then many breaches would likely go unreported. Also, there is no definite timeline in which consumers must be informed, which has been a subject of dispute when Congress was grappling with data security legislation for the better part of this decade. However, when a covered entity notifies a consumer of a breach, it must also give the individual the option to stop the collection, use, retention, sharing or selling of their personal information. Also, consumers must be allowed to require the covered

entity to erase personal information, stop selling and sharing, provide a copy of information the covered entity holds, and close the account and terminate the relationship.

The FTC, state attorneys general, and consumers would all be authorized to bring actions in court for violations of the "Privacy Bill of Rights." The FTC would be required to promulgate regulations that have been discussed at length within one year of enactment, and these regulations would need to take effect within 90 days after being finalized. So, realistically, the FTC would need to produce proposed regulations as quickly as six months after enactment to make the one-year deadline, but, as is customary there is no penalty for the agency missing the deadline. This may be a tall order for the agency given the size of its staff dedicated to privacy and data security issues, many of whom work on the enforcement side, and the resources the agency is provided annually.

Like other privacy bills, the FTC would treat all privacy violations as "a violation of a rule defining an unfair or deceptive act or practice," allowing the agency to seek civil fines of about $42,000 per violation in court as part of its immediate enforcement action. The suite of other enforcement powers would also be available to the FTC including injunctive relief. And, yet, unlike other bills but like Gramm-Leach-Bliley, regulators other than the FTC would be empowered to police violations for their regulators. For example, the federal banking agencies would regulate their sectors of the banking industry.

As mentioned, state attorneys general may enforce the act unless the FTC is already acting. Any actions arising from state laws must be paused until the FTC completes action if both arise from a common set of facts. Notably, this bill does not explicitly preempt state privacy and data security laws. However, under the Constitutional regime of preemption, it is not entirely clear if the "Privacy Bill of Rights" would implicitly preempt state laws, which might be acceptable to privacy and other advocates who may well see this bill as stronger than the "California Consumer Privacy Act" (CCPA) (AB 375).

The bill permits a consumer to sue a covered entity for a violation, a feature rarely included in privacy legislation. An individual could sue in any court of competent jurisdiction, the bill stipulates that "[a] violation of this Act or a regulation promulgated under this Act with respect to the personal information of an individual constitutes an injury in fact to that individual." The latter provision would get consumers over a hurdle they frequently face when they sue regarding data or privacy violations: what is considered an injury necessary to allow a suit proceed. Plaintiffs could seek any of this relief:

(1) actual damages;
(2) punitive damages;
(3) reasonable attorney's fees and costs; and
(4) any other relief, including an injunction, that the court determines appropriate.

Additionally, pre-dispute arbitration agreements shall be null and void as a party to such an agreement will not be able to enforce one, and the court, and not an arbitrator, will determine how this section applies.

Finally, the "Privacy Bill of Rights" would not modify, change, or impinge any other existing privacy laws such Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act, and others.

Senate Appropriators Greenlight Election Security Funds

Key Points:

- *In a sign that the Senate and House may ultimately provide funds for states to secure their election networks in advance of the 2020 election, the Senate bill provides $250 million, some $350 million less than the House would appropriate*
- *The Senate provides a much smaller boost to FTC funding but directs the agency to report on its privacy and security enforcement practices and resources*
- *The FCC would be flat-funded*

Last week, the Senate Appropriations Committee marked up and reported out the bill that funds the Election Assistance Commission, the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and other entities with jurisdiction over technology policy issues. The "Financial Services and General Government Appropriations Act, 2020" (S. 2524) by a 31-0 vote. The Senate is, of course, getting a very late start in moving appropriations bills since Senate Republican leadership blocked all public action on these 12 bills until a deal was struck on the FY 2020 and 2021 budget caps. Such a deal was struck in the "Bipartisan Budget Act of 2019" (P.L. 116-37), and so Senate appropriators were given the greenlight to start marking up bills. In contrast, the House passed the "Financial Services and General Government Appropriations Act, 2020" (H.R. 3551) in June.

In their FY 2020 Financial Services and General Government appropriations package, Senate appropriators would provide $250 million for election assistance grants to states "for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements, as authorized by" the "Help America Vote Act of 2002." The House voted to make $600 million in appropriations, setting up negotiations over a final number. However, given Senate Majority Leader Mitch McConnell's (R-KY) opposition to election security legislation generally, it was not clear whether the Senate Appropriations Committee would allocate any funding for election security.

The Senate would give the FTC $312.3 million, a $2.6 million above the current level of funding. However, the House provided an extra $40 million in FY 2020 for a total of $349.7 million.

The Senate Appropriations Committee included directive language in their committee report pertaining to the FTC and its handling of technology issues:

- Consumer Privacy and Data Security.--The Committee encourages the FTC to use its current authorities to deter unfair and deceptive conduct in consumer privacy and data security matters. Specifically, the Committee encourages the FTC to utilize its Section 5 unfairness authority to distinguish between privacy practices that provide benefits to consumers, and those that are harmful; between those that are fair, and those that are unfair. The Commission is directed to submit a report to the Committee, within 180 days of enactment, on the ways it utilizes its current authorities, including Section 5 unfairness authority, to deter unfair and deceptive conduct in consumer privacy and data security matters.
- Social Media Bots and Deceptive Advertising.--The Committee remains concerned by the increased use of social media bots for advertising purposes and whether their use constitutes a deceptive practice. Bots are becoming increasingly sophisticated, including applying cognitive science techniques to manipulate users into developing trust relationships. Bots are also rapidly expanding in scale, with individuals now able to purchase thousands of bots or fake "followers" to artificially increase their social media standing and potential revenue from advertisements. To assist Congress in better understanding the impact of these advertising practices on consumers, the Committee directs the Commission to submit a report,

not later than 9 months after enactment of this act, describing the growing social media bot market as well as the use of social media bots in online advertising. The report shall include a discussion of how their use might constitute a deceptive practice.

- Social Media and Algorithmic Bias.--Social media has fundamentally democratized Americans' ability to participate in civic discourse. However, while individuals are responsible for the creation of social media content, complex algorithms often determine the distribution, promotion, and placement of that content. This gives rise to the risk that any political biases in these algorithms whether implicit or explicit; intentional or unintentional--leave social media users with a false understanding of the context of the information they receive. The Committee directs the FTC to submit a report, not later than 9 months after enactment of this act, describing the use of algorithms in the distribution of social media content, including an assessment of whether such algorithms are subject to political biases. The report shall include a discussion of how their use might constitute a deceptive practice.
- Technical Expertise.--The Committee is concerned that the FTC lacks sufficient technical expertise to enforce consumer protection in the digital domain. The Committee encourages the FTC's Bureau of Consumer Protection to hire additional technologists to work across the five law enforcement areas (Privacy and Identity Protection, Financial Practices, Marketing Practices, Advertising Practices, and Enforcement). These technologists should have an academic or professional background in computer science, cybersecurity, software engineering or other related field.
- Resources for Data Privacy and Security.--The Committee urges the FTC to conduct a comprehensive internal assessment measuring the agency's current efforts related to data privacy and security while separately identifying all resource-based needs of the FTC to improve in these areas. The Committee also urges the FTC to provide a report describing the assessment's findings to the Committee within 180 days of enactment.

Senate appropriators would flat-fund the Federal Communications Commission (FCC) at $339 million, its current funding level, but so do the House appropriators, suggesting this will be the final figure for the FCC in FY 2020. The Senate Appropriations Committee is directing the FCC to address broadband on tribal lands:

> The Committee remains concerned about the lack of access to broadband services on Tribal lands given the FCC has recently reported additional work remains to increase deployment to certain Tribal areas to reach the Commission's goal of closing the digital divide. The Committee urges the FCC to responsibly and efficiently take action to increase access to broadband on Tribal lands and supports consultation with federally recognized Indian Tribes, Alaska Native villages and corporations, and entities related to Hawaiian home lands. The FCC is encouraged to use all available resources with the goal of spending $300,000 to support consultation with federally recognized Indian tribes, Alaska Native villages, and entities related to Hawaiian home lands. Any action by the FCC to address broadband services on Tribal lands should be done in a manner that takes into account duplication of Federal programs, grants, funding streams, and overbuilding of networks. The FCC should consult with Federal stakeholders and agencies who have a role in deploying broadband when assessing duplication.

Finally, the Senate Appropriations Committee addressed Chinese information and communications technology (ICT):

> Foreign adversaries are seeking to lay the groundwork for the cyber battles of the future by embedding their technologies in systems we depend on. The United States should take proactive steps to deny foreign government access to our networks, sensitive data, and the personal information of the American people. In particular, the Committee remains concerned about the growing national security threat posed by Chinese telecommunications components embedded in networks, systems, and devices that we rely on for critical infrastructure and our daily lives. Therefore, the Committee continues to support the ban included in section 889 of Public Law 115-232 that prohibits government agencies from buying certain telecommunications and video surveillance services or equipment [i.e. Huawei, ZTE, and possibly other Chinese ICT.]

Senate Commerce Hearing on The Relationship Between Social Media and Extremism

Key Points:

- *Facebook, Twitter, and Google discussed the steps they take to combat extremism on their platforms, but none ask for or discuss a federal role in these efforts beyond law enforcement assistance*
- *Member generally approached the issues with the mindset that social media platforms could be doing more but split on the role that stronger gun control laws plays*
- *Legislative solutions were not discussed, generally*

On September 18, the Senate Commerce, Science, and Transportation Committee held a hearing titled "Mass Violence, Extremism, and Digital Responsibility," Members delved into the issues arising from how social media are addressing the extremism and violence that appears on their platforms against the backdrop of threats of some in Congress to remove the liability shield of Section 230 of the Communications Act and a renewed push for gun control legislation. Also operating in the background were recent Republican assertions that social media platforms unfairly censor right-wing points of view.

The witnesses called before the committee were:

- Facebook Head of Global Policy Management Monika Bickert
- Twitter Public Policy Director Nick Pickles
- Anti-Defamation League Senior Vice President of Programs George Selim
- Google Global Director of Information Policy Derek Slater

Chair Roger Wicker (R-MS) acknowledged that "[o]pen platform providers like Google, Twitter, and Facebook and products like Instagram and YouTube have dramatically changed the way we communicate and have been used positively in providing spaces for like-minded groups to come together and in shedding light on despotic regimes and abuses of power throughout the world." He said that "[n]o matter how great the benefits to society these platforms provide, it is important to consider how they can be used for evil at home and abroad." Wicker noted that the El Paso shooter "posted a manifesto to a website called "8chan" 27 minutes prior to the shooting." He said that "[f]ollowing the shooting, President Trump called on social media companies to work in partnership with local, state, and federal agencies to develop tools that can detect mass shooters before they strike – I certainly hope we talk about that challenge today." Wicker reference3d other incidents of "mass violence with an online dimension" such as "shootings at two mosques in Christchurch, New Zealand…[and] [t]he 2016 shooting at the Pulse Nightclub in Orlando, Florida."

Wicker asserted that "[w]ith over 3.2 billion internet users, this committee recognizes the challenge facing social media companies and online platforms' their ability to act and remove content threatening violence from their sites." He said that "[t]here are questions about tracking of a user's online activity, does this invade an individual's privacy, thwart due process, or violate constitutional rights." Wicker contended that "[t]he automatic removal of threatening content may also impact an online platform's ability to detect possible warning signs…[and] the First Amendment offers strong protections against restricting certain speech, this undeniably adds to the complexity of our task."

Wicker said that "[i]n today's internet-connected society, misinformation, fake news, deepfakes, and viral online conspiracy theories have become the norm…[and] [t]his hearing is an opportunity for witnesses to discuss how their platforms go about identifying content and material that threatens violence and poses a *real* and potentially immediate danger to the public." He expressed his hope "our witnesses will also discuss how their content moderation processes work…[which] includes addressing how human review or technological tools are employed to remove or otherwise limit violent content before it is posted, copied, and disseminated across the internet." Wicker said the committee "would like to know how companies are coordinating with law enforcement when violent or extremist content is identified…[and] I hope witnesses will discuss how Congress can assist ongoing efforts to remove content promoting violence from online platforms and whether best practices or industry codes of conduct in this area would help increase safety both online and offline."

Ranking Member Maria Cantwell (D-WA) declared that "[a]cross the country, we are seeing and experiencing a surge of hate and as a result we need to think much harder about the tools and resources we need to combat this problem both online and offline." She said that "[w]hile the First Amendment to the Constitution protects free speech, speech that incites eminent violence is not protected and Congress should review and strengthen laws that prohibit threats of violence, harassment, stalking, and intimidation to make sure that we stop the online behavior that does incite violence." Cantwell cited the testimony of FBI Director Christopher Wray before the committee in which he claimed "white supremacist violence is on the rise." She noted a number of white supremacist violence in Washington state, and "[t]he rise in hate across the country has also led to multiple mass shootings, including the Tree of Life congregation in Pittsburgh, the Pulse nightclub in Orlando and most recently, the Walmart in El Paso."

Cantwell remarked on how social media can amplify hate and serve as a platform for those intent on perpetuating hatred and spreading violence. She said "[t]his is a particular problem on the dark web, where we see certain websites like 8chan and a host of 24/7, 365 hate rallies." Cantwell claimed that "[a]dding technology tools to mainstream websites to stop the spread of these dark websites is a start, but there needs to be more to be a concentrated and coordinated effort to ensure that people are not directed into these cesspools." She added that "I believe calling on the Department of Justice to make sure that we are working across the board on an international basis with companies as well to fight this issue is an important thing to be done." She cautioned that "[w]e don't want to push people off of social media platforms only to then being on the dark web, where we are finding less of them…[and] [w]e need to do more, the Department of Justice, to shut down these dark web sites and social media companies need to work with us to make sure that we are doing this."

Cantwell noted "[t]he state of Washington has passed three initiatives, gun initiatives, by the vote of the people, closing background loopholes and also relating to private sales and extreme person laws, all voted on by a majority of people in our state and have successfully passed." She added

that "I do appreciate, just last week representatives from various companies of all sizes in the tech industry sending the Senate a letter, asking for passage of bills requiring extensive background checks." Cantwell said that "we look forward to asking you about ways in which we can better fight these issues…[and] I do want us to think about ways in which we can all work together to address these issues."

Facebook Head of Global Policy Management Monika Bickert "outline[d]…several of the important steps that we take to prevent violence and keep our users safe:

- Prohibition Against Violence and Incitement: We care deeply about our users and we want them to be safe. Therefore, it is critical to our mission to help prevent potential offline harm that may be related to content on Facebook. We remove content, disable accounts, and work with law enforcement when we believe there is a risk of physical harm or direct threats to public safety.
- Prohibition of Dangerous Individuals and Organizations: In an effort to prevent and disrupt real-world harm, we do not allow any individuals or organizations that proclaim a violent mission, advocate violence, or are engaged in violence to have a presence on Facebook for any purpose, even if it appears benign. This includes organizations or individuals involved in the following:
    - Terrorist activity, both domestic and international;
    - Organized hate, including white supremacy and white nationalism;•Human trafficking; and
    - Organized violence or criminal activity.
    - We do not allow propaganda or symbols that represent any of these organizations or individuals to be shared on our platform unless they are being used to condemn or inform—for example, by media organizations. We do not allow content that praises any of these organizations or individuals or any acts committed by them. And we do not allow coordination of support for any of these organizations or individuals or any acts committed by them.
- No Promoting or Publicizing Crime: We prohibit people from promoting or publicizing violent crime, theft, and/or fraud because we do not want to condone this activity and because there is a risk of copycat behavior. We also do not allow people to depict criminal activity or admit to crimes they or their associates have committed.
- Policies Against Coordinating Harm: In an effort to prevent and disrupt real-world harm, we prohibit people from facilitating or coordinating future activity, criminal or otherwise, that is intended or likely to cause harm to people, businesses, or animals. People can draw attention to harmful activity that they may witness or experience as long as they do not advocate for or coordinate harm.
- 3 Combatting Suicide and Self-Injury: We also use and continue to develop tools and resources to proactively identify and help people who may be at risk of suicide or self-injury. We leverage pattern recognition technology to detect posts or live videos where someone might be expressing an intent to harm themselves. We also use artificial intelligence (AI) to prioritize the order in which our team reviews reported content relating to suicide or self-injury. This ensures we can get the right resources to people in distress and, where appropriate, we can more quickly alert first responders. And we remove content that encourages suicide or self-injury, including certain graphic imagery and real-time depictions that experts tell us might lead others to engage in similar behavior. We also work with organizations around the world to provide assistance and resources to people in distress.
- Cooperation with Law Enforcement: Law enforcement plays a critical role in keeping people safe, and we have a long history of working successfully with law enforcement to address

a wide variety of threats. As a former federal prosecutor, I know that this cooperation is vital. When we do receive reports or otherwise find content that violates our policies, we remove it. And we proactively reach out to law enforcement if we see a credible threat of imminent harm.

Twitter Public Policy Director Nick Pickles explained that "[a]ll individuals accessing or using Twitter's services must adhere to the policies set forth in the Twitter Rules." He said that "[a]ccounts under investigation or that have been detected as sharing content in violation with the Twitter Rules may be required to remove content, or in serious cases, will see their account permanently suspended…[and] [o]ur policies and enforcement options evolve continuously to address emerging behaviors online:

- A. Policy on Terrorism Individuals on Twitter are prohibited from making specific threats of violence or wish for the serious physical harm, death, or disease of an individual or group of people. This includes, but is not limited to, threatening or promoting terrorism. We suspended more than 1.5 million accounts for violations related to the promotion of terrorism between August 1, 2015, and December 31, 2018. In 2018, a total of 371,669 accounts were suspended for violations related to promotion of terrorism. More than 90 percent of these accounts are suspended through our proactive measures. We have a zero-tolerance policy and take swift action on ban evaders and other forms of behavior used by terrorist entities and their affiliates.
- B. Policy on Violent Extremist Groups In December 2017, we broadened our rules to encompass accounts affiliated with violent extremist groups. Our prohibition on the use of Twitter's services by violent extremist groups — i.e., identified groups subscribing to the use of violence as a means to advance their cause —applies irrespective of the cause of the group. Our policy states: Violent extremist groups are those that meet all of the below criteria:
    - identify through their stated purpose, publications, or actions as an extremist group;
    - have engaged in, or currently engage in, violence and/or the promotion of violence as a means to further their cause; and
    - target civilians in their acts and/or promotion of violence.An individual on Twitter may not affiliate with such an organization — whether by their own statements or activity both on and off the service — and we will permanently suspend those who do so.
- C. Policy on Hateful Conduct People on Twitter are not permitted to promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease. We also do not allow accounts whose primary purpose is inciting harm toward others on the basis of these categories. We do not allow individuals to use hateful images or symbols in their profile image or profile header. Individuals on the platform are not allowed to use the username, display name, or profile bio to engage in abusive behavior, such as targeted harassment or expressing hate toward a person, group, or protected category. Under this policy, we take action against behavior that targets individuals or an entire protected category with hateful conduct. Targeting can happen in a number of ways, for example, mentions, including a photo of an individual, or referring to someone by their full name.
- D. Investing in Tech: Behavior vs. Content Twitter's philosophy is to take a behavior-led approach, utilizing a combination of machine learning and human review to prioritize reports and improve the health of the public conversation. That is to say, we increasingly look at how accounts behave before we look at the content they are posting. This is how we

seek to scale our efforts globally and leverage technology even where the language used is highly context specific. Twitter employs extensive content detection technology to identify potentially abusive content on the service, along with allowing users to report content to us either as an individual or a bystander .For abuse, this strategy has allowed us to take three times the amount of enforcement of action on abuse within 24 hours than this time last year. We now proactively surface over 50percent of abusive content we remove using our technology compared to 20 percent a year ago. This reduces the burden on individuals to report content to us.

Anti-Defamation League Senior Vice President of Programs George Selim made a number of detailed policy recommendations to counter the threat posed by extremism as it presents online:

1. Bully Pulpit. The President, cabinet officials, and Members of Congress must call out bigotry at every opportunity. The right to free speech is a core value, but the promotion of hate should be vehemently rejected. Simply put, you cannot say it enough: America is no place for hate.
2. Enforcement of Existing Laws. The Administration must send loud, clear, and consistent messages that violent bigotry is unacceptable and ensure that the FBI and the Justice Department's Civil Rights Division will enforce relevant federal laws and vigorously investigate and prosecute hate crimes.
3. Improve Federal Hate Crime Training and Data Collection. The Department of Justice should incentivize and encourage state and local law enforcement agencies to more comprehensively collect and report hate crimes data to the FBI, with special attention devoted to large underreporting law enforcement agencies that either have not participated in the FBI Hate Crime Statistics Act program at all or have affirmatively and not credibly reported zero hate crimes. More comprehensive, complete hate crime reporting can deter hate violence and advance police-community relations.
4. Legislation to Address White Supremacy and Domestic Terrorism. Congress must act to counter the threat of domestic terrorism and prevent more attacks. No legislative action is perfect, but inaction should not be an option. Congress should enact the following measures:
    - Domestic Terrorism Prevention Act (DTPA) (S. 894/ HR 1931). This legislation would enhance the federal government's efforts to prevent domestic terrorism by authorizing into law the offices addressing domestic terrorism, and would require federal law enforcement agencies to regularly assess those threats. The bill would also provide training and resources to assist non-federal law enforcement in addressing these threats, requiring DOJ, DHS, and the FBI to provide training and resources to assist state, local, and tribal law enforcement in understanding, detecting, deterring, and investigating acts of domestic terrorism.
    - Domestic Terrorism Documentation and Analysis of Threats in America (DATA) Act (HR 3106). Data on extremism and domestic terrorism is being collected by the FBI, but not enough, and the reporting is insufficient and flawed. Data drives policy; we cannot address what we are not measuring. The DATA Act focuses on increasing the coordination, accountability, and transparency of the federal government in collecting and recording data on domestic terrorism.
    - The Khalid Jabara and Heather Heyer National Opposition to Hate, Assault, and Threats to Equality Act of 2019 (NO HATE Act of 2019 S. 2043/ H.R. 3545). This legislation would authorize incentive grants to spark improved local and state hate crime training, prevention, best practices, and data collection initiatives –including grants for state hate crime reporting hotlines to direct individuals to local law enforcement and support services.

- Disarm Hate Act (S.1462/H.R.2708). This legislation would close the loophole that currently permits the sale of firearms to individuals who have been convicted of threatening a person based on their race, religion, gender, sexual orientation, or disability. The measure would prohibit individuals convicted of a misdemeanor hate crime from obtaining a firearm.
- In addition, more consideration is needed for two additional initiatives that could help address white supremacy and domestic terrorism in the United States.
    - Congress should examine whether a rights-protecting domestic terrorism criminal charge is needed –and could be appropriately crafted. Our federal legal system currently lacks the means to prosecute a white supremacist terrorist as a terrorist. Perpetrators can be prosecuted for weapons charges, acts of violence (including murder), racketeering, hate crimes, or other criminal violations. But we cannot legally prosecute them for what they are: terrorists.
    - The State Department should examine whether certain white supremacist groups operating abroad meet the specific criteria to be subject to sanctions under its Designated Foreign Terrorist Organization (FTO) authority.T he criteria, set out in 8 U.S.C. § 1189(a) are: (1) the organization must be foreign; (2) the organization must engage in terrorist activity or retain the capability and intent to engage in terrorist activity or terrorism; and (3) the terrorist activity or terrorism of the organization must threaten the security of U.S. nationals or the national security of the U.S. None of the current 68 organizations on the FTO list is a white supremacist organization.
    - Second, in the United States, unlike in Canada and England, the First Amendment provides unique, broad protection for even the most vile hate speech and propaganda. While clearly criminal conduct would not be protected under the First Amendment, a great deal of non-criminal association, speech, and hateful propaganda would be protected speech. The First Amendment's assembly and speech protections would not permit designation of white supremacist organizations operating here, but designating foreign white supremacist groups could make knowingly providing material support or resources to them a crime –extending authority for law enforcement officials to investigate whether such a crime is being planned or is occurring.

5. Address Online Hate and Harassment

- Strengthen laws against perpetrators of online hate. Hate and harassment translate from real-world to online spaces, including in social media and games, but our laws have not kept up. Many forms of severe online misconduct are not consistently covered by cybercrime, harassment, stalking and hate crime law. Congress has an opportunity to lead the fight against cyberhate by increasing protections for targets as well as penalties for perpetrators of online misconduct.
- Urge social media platforms to institute robust governance. Government officials have an important role to play in encouraging social media platforms to institute robust and verifiable industry-wide self-governance. This could take many forms, including Congressional oversight or passing laws that require certain levels of transparency and auditing. The internet plays a vital role in allowing for innovation and democratizing trends, and that should be preserved. At the same time the ability to use it for hateful and severely harmful conduct needs to be effectively addressed.

- Improve training of law enforcement. Law enforcement is a key responder to online hate, especially in cases when users feel they are in imminent danger. Increasing resources and training for these departments is critical to ensure they can effectively investigate and prosecute cyber cases and that targets know they will be supported if they contact law enforcement.

6. Platform Responsibility to Address Online Hate and Harassment
    - Terms of Service. Every social media and online game platform must have clear terms of service that address hateful content and harassing behavior, and clearly define consequences for violations.
    - Responsibility and Accountability. Social media and online game platforms should assume greater responsibility to enforce their policies and to do so accurately at scale. They should improve the complaint and flagging process so that it provides a more consistent and speedy resolution for targets.
    - Governance and Transparency. Perhaps most importantly, social media and online game platforms should adopt robust governance. This should include regularly scheduled external, independent audits so that the public knows the extent of hate and harassment on a given platform. Audits should also allow the public to verify that the company followed through on its stated actions and assess the effectiveness of company efforts over time. Companies should provide information from the audit and elsewhere through more robust transparency reports. Finally, companies should create independent groups of experts from relevant stakeholders, including civil society, academia and journalism, to help provide guidance and oversight of platform policies.

Industry Groups Press Congress on Federal Privacy Legislation

Key Points:

- *Industry groups turn to Congress on privacy legislation after efforts to amend the CCPA fall short in Sacramento*
- *Three industry groups release public statements calling for passage of a federal data privacy law that would preempt the CCPA and other state laws*

As it became clear that efforts to amend the "California Consumer Privacy Act" (CCPA) (AB 375) were going to fall short of what industry groups and other stakeholders wanted, three industry trade groups called on Congress to enact federal privacy legislation that would preempt California and other states with privacy laws. A number of key Members of Congress said before the August recess that they would be unveiling their proposals in September; however, no such legislation has been released. Additionally, with the CCPA set to take effect on January 1, 2020 and California Attorney General Xavier Becerra set to release draft CCPA regulations, lawmakers on Capitol Hill may be feeling pressure to act.

TechNet, a "national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy," issued a statement:

> Actions taken by the California Legislature this year will improve the California Consumer Privacy Act, but many clarifications are still necessary before it will work for consumers and businesses. Any privacy law should put consumers first and ensure businesses can comply with the law while continuing to innovate. Unfortunately, California's privacy law in its current form falls short of these critical benchmarks. While we hope the rulemaking process

> will allow for additional improvements, the importance of federal action to avoid a patchwork of privacy laws has never been clearer, and we urge Congress to act.

Of note, TechNet speaks about preemption in the familiar terms of avoiding numerous, different laws (i.e. a patchwork). Also, the organization makes clear its disappointment that the California legislature did not fix the bill as it had hoped.

Also this month, the Internet Association (IA) association launched the "Privacy For All Americans" campaign:

> Internet companies believe all Americans should have comprehensive federal privacy protections that give them control over the data they provide to companies across all industries, regardless of where they live. That includes having the ability to access, correct, delete, and download their data. The time is now for Congress to pass a comprehensive, federal privacy law that establishes a consistent nationwide standard and reflects an American approach to privacy.

IA bills itself as "the only trade association that exclusively represents leading global internet companies on matters of public policy."

Like TechNet, IA does not use terminology like preemption; rather, they urge Congress to enact a "comprehensive" statute that creates a "consistent nationwide standard." While IA calls for consumers to be able "to access, correct, delete, and download their data," the statement is silent on other features of privacy legislation. In its "Privacy Principles For A Modern National Regulatory Framework" released last year, IA spells out more clearly its positions on privacy legislation, including its explicit support for preemption and risk-based approach that set performance benchmarks instead of proscribing practices.

Earlier this month, 51 corporate CEOs signed a Business Roundtable letter urging Congress "to pass, as soon as possible, a comprehensive consumer data privacy law that strengthens protections for consumers and establishes a national privacy framework to enable continued innovation and growth in the digital economy." They asserted that "[w]e urgently need a comprehensive federal consumer data privacy law to strengthen consumer trust and establish a stable policy environment in which new services and technologies can flourish within a well-understood legal and regulatory framework. Innovation thrives under clearly defined and consistently applied rules." The letter was addressed to the four Congressional leaders and the chairs and ranking members of the House Energy and Commerce and Senate Commerce, Science and Transportation Committees.

This letter comes at a time when stakeholders claimed they would have developed and introduced legislation to establish federal privacy standards. A number of key Members said before the August recess that they would be unveiling their proposals in September; however, no such legislation has been released. Additionally, with the "California Consumer Privacy Act" (CCPA) (AB 375) set to take effect on January 1, 2020 and California Attorney General Xavier Becerra set to release draft CCPA regulations, lawmakers on Capitol Hill may be feeling pressure to act.

The CEOs claimed that "[t]here is now widespread agreement among companies across all sectors of the economy, policymakers and consumer groups about the need for a comprehensive federal consumer data privacy law that provides strong, consistent protections for American consumers." They stated that "[a] federal consumer privacy law should also ensure that American companies

continue to lead a globally competitive market…[and] [w]e are committed to protecting consumer privacy and want consumers to have confidence that companies treat their personal information responsibly." The CEOs said that "[w]e are also united in our belief that consumers should have meaningful rights over their personal information and that companies that access this information should be held consistently accountable under a comprehensive federal consumer data privacy law."

However, the CEOs made the case for a federal privacy statute to preempt the CCPA and other state laws. They claimed that "[c]onsumers should not and cannot be expected to understand rules that may change depending upon the state in which they reside, the state in which they are accessing the internet, and the state in which the company's operation is providing those resources or services." The CEOs added that "[n]ow is the time for Congress to act and ensure that consumers are not faced with confusion about their rights and protections based on a patchwork of inconsistent state laws." The CEOs stated that "as the regulatory landscape becomes increasingly fragmented and more complex, U.S. innovation and global competitiveness in the digital economy are threatened."

Late last year, the Business Roundtable Framework for Consumer Privacy Legislation in which the organization more fully articulated its views on what federal privacy legislation should look like. Not surprisingly, the organization favors complete federal preemption and no private right of action for consumers to sue. Additionally, the Business Roundtable seems not to prefer that the Federal Trade Commission (FTC) not be given a freer rein to fine violators. They asserted "[e]nforcement actions and fines should be informed by the harm directly caused by, and severity of, an organization's conduct as well as any actions taken by the organization to avoid and mitigate the harm, the degree of intentionality or negligence involved, degree of cooperation, and the organization's previous conduct involving personal data privacy and security."

GAO Finds DOD Failed To Meet Statutory Requirements on Open Source Software

Key Points:

- *Contrary to direction in the FY 2018 NDAA, the Pentagon failed to fully implement an Obama Administration initiative to give federal agencies more control over software developed for government use*
- *The DOD agreed to take the steps identified by GAO*

The Government Accountability Office (GAO) evaluated how well the Department of Defense (DOD) is meeting an Office of Management and Budget (OMB) directive for agencies to implement open source software (OSS) pilots. The GAO was required to report on the DOD's OSS pilot per the FY 2018 National Defense Authorization Act (NDAA), which also required the DOD to implement such a program. The OMB directive applied only to civilian agencies and systems, making most of the DOD exempt. Congress decided to include the DOD with language in the NDAA.

In M-16-21, OMB sought to ensure "that new custom-developed Federal source code be made broadly available for reuse across the Federal Government…consistent with the Digital Government Strategy's "Shared Platform" approach, which enables Federal employees to work together—both within and across agencies—to reduce costs, streamline development, apply uniform standards, and ensure consistency in creating and delivering information." OMB added that "[e]nhanced reuse of custom-developed code across the Federal Government can have significant benefits for American taxpayers, including decreasing duplicative costs for the same code and reducing Federal vendor lock-in." However, "national security systems" (i.e. most of the DOD and

the Intelligence Community) were exempt from this memorandum. As noted, the FY 2018 NDAA specifically directed the DOD to implement the OSS initiative.

The GAO found that the "DOD has not fully implemented an open source software pilot program and related OMB requirements as mandated by the [FY 2018 NDAA]." The GAO explained that "OMB memorandum M-16-21 calls for agencies to implement a pilot program, which it defines as

(1) releasing at least 20 percent of new custom developed code as open source, and
(2) establishing a metric for calculating program performance.

The GAO determined that "DOD has not fully implemented the program and has not established the metric."

The GAO stated that "[t]he OMB memorandum also requires agencies to implement other supporting activities…[and] [t]hese include issuing policy on government-wide use of code, conducting analyses of software solutions, securing data rights and inventory code, and facilitating the open source community." The GAO found that "DOD has not implemented the policy requirement and has partially implemented the remaining three requirements:"

- Regarding the policy and analysis requirements, DOD plans to issue a policy and conduct analyses by the end of the 2019 calendar year. If the department effectively implements these intended steps consistent with OMB direction, DOD should be able to fully address these requirements.
- For the requirement of securing data rights and inventorying code, DOD issued a memorandum that directs contracting officers to secure data rights and to identify all source code created after August 2016. However, DOD's components have not executed these activities nor has DOD identified a milestone for when they will be completed.
- For the facilitating community requirement, DOD issued a memorandum that encourages conversations to foster communities and allow others to contribute knowledge, among other initiatives. However, DOD has not fully engaged in open development, established a release schedule, or fully documented its source code to facilitate use and adoption. To address these areas, DOD's Chief Information Officer plans to issue guidance but has not established a milestone for doing so.

The GAO noted that DOD Is failing to meet the requirements set out in the FY 2018 NDAA to meet OMB's requirements. Yet, GAO noted that "DOD officials from 11 components expressed their opinions that an open source pilot program would potentially result in financial benefits and increased efficiency…[and] there were disparate views on how to manage the cybersecurity risk of using open source software." The GAO stated that "officials from three components noted that security concerns could result in the sporadic use of OSS, whereas eight officials stated that the potential cybersecurity risks were manageable."

The GAO recommended that the DOD take the following steps:

- The Secretary of Defense should ensure the department implements the pilot program by releasing at least 20 percent of newly custom- developed code as OSS. (Recommendation 1)
- The Secretary of Defense should ensure the department identifies a measure to calculate the percentage of code released to gauge its progress on implementing the pilot program. (Recommendation 2)

- The Secretary of Defense should ensure the department establishes milestones for completing the requirements of OMB memorandum M- 16-21 of securing data rights and conducting an inventory. (Recommendation 3)
- The Secretary of Defense should ensure the department establishes a milestone for completing the OMB memorandum's requirement of facilitating an OSS community. (Recommendation 4)

Dueling Cyber Working Groups Convene At U.N.

Key Points:

- *Per U.N. resolutions passed last year, two groups have started working on the development of nation-state norms in cyberspace*

Last week, two bodies convened per 2018 United Nations resolutions started meeting to further consultative discussions on an international agreement or set of agreements on what is considered acceptable and unacceptable cyber practices. Previous efforts largely stalled over disagreements between a bloc led by the U.S. and its allies and nations like China, Russia, and others with a different view on acceptable practices. Notably, unlike 2010, 2013 and 2015, the 2017 UN Group of Governmental Experts (GGE) could not reach agreement on additional voluntary, non-binding norms on how nations should operate in cyberspace.

As explained in a 2018 U.N. press release, it was explained that two resolutions to create groups "aimed at shaping norm-setting guidelines for States to ensure responsible conduct in cyberspace:"

- the draft resolution "Developments in the field of information and telecommunications in the context of international security" (document A/C.1/73/L.27.Rev.1), tabled by the Russian Federation. By the text, the Assembly would decide to convene in 2019 an open-ended working group acting on a consensus basis to further develop the rules, norms and principles of responsible behaviour of States.
- the draft resolution "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (document A/C.1/73/L.37), tabled by the United States…[that] would request the Secretary-General, with the assistance of a group of governmental experts to be established in 2019, to continue to study possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States.

The U.N. noted that '[s]everal speakers pointed out that language in [the Russian proposal] departed from previous year's versions and included excerpts from the Group of Governmental Experts reports in a manner that distorted their meaning and transformed the draft resolution." The U.N. also acknowledged that "some delegates said [the U.S. proposal] called for the establishment of a new group of governmental experts, with the same mandate as the previous ones and the same selectivity in terms of its composition." The U.N. added that "[m]ore broadly, while some delegates regretted to note that two separate, yet similar draft resolutions were tabled, others highlighted a need for bold, swift action to prevent cyberattacks and malicious online behaviour."

In the 2018 resolution offered by Russia, an Open-Ended Working Group (OEWG) was convened "with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent…and to further develop the rules, norms and principles of responsible behaviour of States" from previous UN-sponsored efforts. The OEWG was further tasked with examining "the ways for their

implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts." The OEWG is charged with submitting "a report on the results of the study to the General Assembly at its seventy-fifth session, and to provide the possibility of holding, from within voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate."

The U.S. resolution stated its purpose as

> with the assistance of a group of governmental experts, to be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in the above-mentioned reports, to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States, and to submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States…

Trump Administration Announces Plan To Modify Bush-Era Means Of Protecting Federal Networks

Key Points:

- *The Administration releases its plan to move federal agencies from the cybersecurity model of protecting the perimeter to one of segmented, comparted defense*
- *This move dovetails with the Administration's broader push to leverage private cloud offerings to modernize federal IT*
- *DHS will be developing the requirements agencies must meet in transitioning to the new mode*

The Office of Management and Budget (OMB) has released its long-awaited revision to the Trusted Internet Connections (TIC) initiative that is of a piece with the Trump Administration's push to modernize the federal government's information technology (IT), notably by moving as much of operations as possible and feasible to the cloud. The Department of Homeland Security (DHS) will define what constitutes "TIC Use Cases" that will define alternative standards and processes that agencies may ultimately use instead of TIC. To this end, "DHS, in coordination with OMB and the Federal Chief Information Security Officer (CISO) Council shall establish and publicly release a detailed process document."

OMB explained

> The purpose of the TIC initiative is to enhance network security across the Federal Government. Initially, this was done through the consolidation of external connections and

> the deployment of common tools at these access points. While this prior work has been invaluable in securing Federal networks and information, the program must adapt to modern architectures and frameworks for government IT resource utilization. Accordingly, this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.

OMB rescinded four TIC "memoranda [that] required agency traffic to flow through a physical TIC access which has proven to be an obstacle to the adoption of cloud-based infrastructure:"

- M-08-05, Implementation of Trusted Internet Connections (TIC) (November 20, 2007)
- M-08-16, Guidance for TIC Statement of Capability Form (SOC) (April 4, 2008)
- M-08-27, Guidance for TIC Compliance (September 30, 2008)
- M-09-32, Update on the TIC Initiative (September 17, 2009)

In terms of background, the George W. Bush Administration started the TIC initiative, which was intended "to improve the federal government's security posture by reducing and consolidating external network connections, including Internet connections, currently in use by the government, and by centrally monitoring the traffic passing through these connections for potentially malicious activity...[and] [a]lthough the initiative is intended to secure connections to the Internet, other external connections to potentially unsecured systems must also be routed through an approved TIC access point, even if they do not pass through the Internet" as the Government Accountability Office explained in December 2018.

OMB explained why the TIC policy no longer serves the federal government and why it frustrates agencies from moving to the cloud in its Cloud Smart strategy:

> While this initial architectural concept served an important purpose at its inception, at a time when networking was constrained by physical limitations and agency approaches to network security were not standardized and highly fragmented, the technology landscape has evolved to provide agencies with more tools, technologies, and approaches to secure their data, leaving the once-useful TIC construct now relatively inflexible and incompatible with many agencies' requirements. With the proliferation of private-sector cloud offerings, the emergence of software-defined networks, and an increasingly mobile workforce, the TIC model must compete with newer, more flexible solutions that provide equal or greater security, or it must evolve as well.

In response to a question at a March hearing before the House Appropriations Committee's Homeland Security Subcommittee, Cybersecurity and Infrastructure Security Agency (CISA) head Christopher Krebs explained:

> in the traditional or historic on premise environment of having a server room and having a data center where you know where the equipment is and you can really sit on the pipes and focus them down, TIC was important. Going forward, as particularly we shift through IT modernization to cloud because cloud is efficient, it is scalable, it is flexible to meet modern workforce demands, TIC won't work because TIC actually undermines the low latency and high speed and flexibility of the cloud.

In the Report to the President on Federal IT Modernization, the Administration explained

> Under this model, agencies are required to reduce external connections to a target of 50 and route their traffic through this limited number of secure gateways. These gateways apply common security protections, as well as common intrusion detection, information sharing, and prevention capabilities under DHS's National Cybersecurity Protection System (NCPS). NCPS consists of three sensor capabilities, collectively referred to as EINSTEIN, as well as a set of analytic tools used by cyber analysts to find, identify and categorize cyber threat activity.

In the TIC Update, OMB stated that "[t]o continue to promote a consistent baseline of security capabilities, the Department of Homeland Security (DHS) will define TIC initiative requirements in documentation called TIC Use Cases...[that] will outline which alternative security controls, such as endpoint and user- based protections, must be in place for specific scenarios in which traffic may not be required to flow through a physical TIC access point." OMB added that "[t]o promote flexibility while maintaining a focus on security outcomes, the capabilities used to meet TIC Use Case requirements may be separate from an agency's existing network boundary solutions provided by a Trusted Internet Connection Access Provider (TICAP) or Managed Trusted Internet Protocol Services (MTIPS)." OMB stated that "[g]iven the diversity of platforms and implementations across the Federal Government, TIC Use Cases will highlight proven, secure scenarios, where agencies have met requirements for government-wide intrusion detection and prevention efforts, such as the National Cybersecurity Protection System (including the EINSTEIN suite), without being required to route traffic through a TICAP/MTIPS solution."

OMB laid out specific tasks to realize the goals of the TIC Update:

> 1. Within 60 days of the release of this memorandum, DHS, in coordination with OMB and the Federal Chief Information Security Officer (CISO) Council shall establish and publicly release a detailed process document that incorporates the following elements:
>
> a.) Initiate Pilots: The Federal CISO Council shall solicit and review agency and industry TIC pilot proposals on an ongoing basis, participate in the approval process for updates to TIC Use Cases and other TIC reference architecture documentation, and establish the timeline for DHS to review pilot results and approve updates to TIC Use Cases and other TIC documentation;
>
> b.) Manage Pilots: DHS, in coordination with OMB, the General Services Administration (GSA), and the CISO Council shall oversee and support agency TIC pilots, as appropriate;
>
> c.) Approve Use Cases: DHS, in coordination with OMB, GSA, and the CISO Council, shall review pilot results and approve updates to TIC Use Cases and other TIC reference architecture documentation;
>
> d.) Acquisitions: GSA shall update government-wide procurement vehicles, as appropriate, within 6 months of the approval of new TIC Use Case requirements and other TIC reference architecture documentation; and
>
> e.) Collect Feedback: DHS, in coordination with GSA, shall establish a coordinated process for soliciting agency and industry input on approved TIC Use Cases and other TIC reference architecture documentation. DHS will ensure TIC Use Cases and other TIC reference architecture documentation are kept up to date as changes are approved.
>
> 2. Within 90 days of the release of each TIC Use Case, DHS, in coordination with GSA and NIST, shall develop a compliance verification process to validate that agencies are

implementing the security controls required by TIC Use Cases. DHS will update this verification process as necessary to promote continuous improvement.

OMB explained that "agency Chief Information Officers shall maintain an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection in the event OMB, DHS, or others request this information to assist with government-wide cybersecurity incident response or other cybersecurity matters" and articulated this goal:

> 1. Within one year of the release of this memorandum, agencies shall complete updates to their own network and system boundary policies to reflect this memorandum, including guidance regarding potential pilots. Agencies will identify which TIC Use Case will be allowed for the agency. OMB and DHS will track agency implementation through Federal Information Security Modernization Act of 2014 (FISMA) reporting.

ICT Supply Chain Task Force Releases Interim Report

Key Points:

- *An industry-led body submitted its initial findings and recommendations on the U.S. can and should address supply chain risk for information and communications technology (ICT)*
- *This CISA-sponsored effort is working in parallel with two other Administration undertakings to find and exclude risky ICT from federal and key private sector systems and networks*

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has released the interim report of the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (Task Force). This Task Force's work may inform two other parallel efforts to address U.S. supply chain risk for ICT, one mandated by Congress, and the other launched by the Trump Administration via executive order. Of course, this Task Force had broad private sector participation and input, and there will likely be future activities and output from this body.

The Task Force was established in October 2018 "with strategic mandates to provide a forum for the collaboration of private sector owners and operators of ICT critical infrastructure and to provide advice and recommendations to DHS on means for assessing and managing risks associated with the ICT supply chain." The Task Force explained that it had been "[c]hartered under the National Infrastructure Protection Plan Framework and the associated Critical Infrastructure Partnership Advisory Council (CIPAC)" and that its "efforts are directed by a collaborative leadership team with representatives from DHS and the Communications and Information Technology Sectors."

The Task Force stated that its "constituent Working Groups (WG) are comprised of sector members, subject matter experts from those sectors, and representatives from across the Federal Government." The Task Force stated that "[e]ach of the four Working Groups established in the first phase of the Task Force addressed a specific issue area:

- Working Group #1: Information Sharing – Development of a common framework for the bi-directional sharing of actionable supply chain risk information across the community.
- Working Group #2: Threat Evaluation – Identification of processes and criteria to better understand and evaluate threats to ICT supplies, products, and services.
- Working Group #3: Qualified Bidder Lists and Qualified Manufacturer Lists (QBL/QML) – Identification of market segments and evaluation criteria to establish Qualified Bidder and

Qualified Manufacturer Lists that address considerations of vendor and product inclusion and exclusion.

- Working Group #4: Policy Recommendations to Incentivize Purchase of ICT from Original Equipment Manufacturers (OEM) & Authorized Resellers – Policy recommendations principally aimed at stopping the growing problem of counterfeit ICT procurement.

In the interim report, the Task Force provided summaries of what the WGs had achieved:

- **Working Group 1**
  - WG1 determined that many types of risk information are available, but the sources were little known, not affordable, or not easily accessible. Since the threats to the supply chain are varied and diverse, no single repository of supply chain risk information can accommodate all facets of supply chain risk. As such, accessing and utilizing risk information is resource-intensive and, consequently, must be prioritized based on risk.
  - Upon additional review and analysis of the supply chain threat vectors, WG1 observed that the information of highest value in mitigating risk pertains to suspected, known, and/or proven bad actors. Correspondingly valuable information relates to specific threats to information technology/operational technology products, software, or services. WG1 sought to determine where this valuable information resided, noting that the most likely sources of information that could identify "suspect" supplier behavior would be drawn from primarily industry sources.
  - While there are some mechanisms in place for industry to disclose suspect supplier behavior, legal issues have been identified in sharing and/or receiving potentially derogatory, supplier-specific information.
  - This remains an open issue about which WG 1 has not formed any conclusions.
- **Working Group 2**
  - WG 2 developed a "Threat List [that] was carefully broken down into nine categories that provide the framework for the threats and guided the inputs of the members:
    - Counterfeit Parts
    - Cybersecurity
    - Internal Security Operations and Controls
    - Compromise of System Development Life Cycle (SDLC) Processes and Tools
    - Insider Threat
    - Inherited Risk (Extended Supply Chain)
    - Economic
    - Legal
    - External End-to-End Supply Chain
- **Working Group 3**
  - WG3 developed a draft deliverable report that includes discussion of approaches to supply chain assurance, examples of current supply assurance programs, and recommended next steps. Completing the inventory and publishing the initial guidance from WG2 are the prerequisites for WG3 to ensure that identified key gaps are addressed through policy recommendations.
- **Working Group 4**
  - WG4 delivered a policy recommendation that ICT be purchased from original manufacturers or their authorized resellers. The policy recommendation, fully titled Procurement of Information and Communications Technology from Original Equipment Manufacturers, their Authorized Channels, or other Trusted Supplier(s),

> incorporates a number of definitions circumscribing the term "authorized reseller" which include specific cyber and supply chain security requirements, informed by leading industry practices, the DFARS rule, commercial standards such as SAE AS6496 (Authorized Distributor Anti-Counterfeiting Standard), and ISO/IEC 20243 (Information Technology -- Open Trusted Technology Provider Standard (O-TTPS)). After the recommendation was unanimously agreed to by the Task Force Executive Committee, it was subsequently transmitted to the Federal Acquisition Security Council (FASC).

As noted, this Task Force stands aside and apart from other parallel, sometimes overlapping efforts of the Trump Administration to address ICT supply chain risk.

The recently established FASC has begun meeting. As you may recall, this body was created in an end-of-the-year bill, the "Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act" (SECURE Act) (P.L. 115-390), that charged with the new body with a number of responsibilities, including:

- developing an information sharing process for agencies to circulate decisions throughout the federal government made to exclude entities determined to be IT supply chain risks
- recommending orders applicable to executive agencies requiring the exclusion of sources or covered articles from executive agency procurement actions (exclusion orders) establishing a process by which entities determined to be IT supply chain risks may be excluded from procurement government-wide (exclusion orders) or suspect IT must be removed from government systems (removal orders)
- creating an exception process under which IT from an entity subject to a removal or exclusion order may be used if warranted by national interest or national security
- issuing recommendations for agencies on excluding entities and IT from the IT supply chain and "consent for a contractor to subcontract" and mitigation steps entities would need to take in order for the Council to rescind a removal or exclusion order

And, yet this body has not yet released any proposals or materials for public input. Nonetheless, in June remarks at an industry event, four weeks after its first meeting, Federal Chief Information Security Officer (CISO) Grant Schneider identified the FASC's priorities:

- developing standards on how agencies develop for supply chain;
- identifying an information sharing agency within the government;
- creating shared services around supply chain;
- and creating criteria and implementing recommendations for different agencies within the Federal enterprise.

In May 2019, the President issued Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," that declared a national emergency on the basis that

> the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

Most relevant to the Task Force's work, the EO tasks DHS with "produc[ing] a written assessment within 80 days of the date of this order, and annually thereafter...[that] shall include an evaluation of hardware, software, or services that are relied upon by multiple information and communications technology or service providers, including the communication services relied upon by critical infrastructure entities."

More broadly, the EO prohibits the following:

> any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service), where the transaction was initiated, is pending, or will be completed after the date of this order [subject to a determination from the Secretary of Commerce]

Accordingly, in order to actually ban any ICT, the Department of Commerce, in consultation with a number of other agencies, must determine

> (i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
> (ii) the transaction:
>> (A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;
>> (B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
>> (C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

Moreover, by October 12, 2019, the Department of Commerce must promulgate regulations to implement this portion of the EO.

However, at least according to a June 2019 Task Force press statement, there is coordination between these efforts: "The Task Force also discussed best mechanisms for providing input into the recently launched Federal Acquisition Security Council and its role in assisting in DHS' analytical requirements laid out in the May 15th Executive Order on Securing the Information and Communications Technology and Services Supply Chain."

CFIUS Regulations

Key Points:

- *Draft regulations would implement expansion of the CFUIS process enacted into law last year by lawmakers concerned about Chinese efforts to buy U.S. firms or technology in key sectors*

The Department of the Treasury issued draft regulations to implement a statutorily required update and expansion of the process by which the U.S. government determines whether to allow a foreign

entity to purchase controlling interest in a U.S. company if the deal has national security implications. The FY 2019 National Defense Authorization Act (NDAA) (P.L. 115-32) contained a significant rewrite of the Committee on Foreign Investment in the United States (CFIUS) process in the "Foreign Investment Risk Review Modernization Act of 2018" (FIRRMA). These provisions would give the inter-agency process more latitude, tools, and direction in evaluating deals with national security implications, particularly in light of the People's Republic of China's ambitions to displace the U.S. in a number of existing technology fields and to take the lead in a number of cutting-edge fields. Notably, should a company or entity seek less than a controlling interest, it may be subject to the CFIUS process and now CFIUS may take into account "critical technologies," "critical infrastructure," or "sensitive personal data" when evaluating transactions.

In a Treasury fact sheet, the agency explained that "FIRRMA expands CFIUS's jurisdiction beyond transactions that could result in foreign control of a U.S. business to also include a non-controlling investment, direct or indirect, by a foreign person that affords the foreign person:

- access to any material nonpublic technical information in the possession of the U.S. business;
- membership or observer rights on the board of directors or equivalent governing body of the U.S. business or the right to nominate an individual to a position on the board of directors or equivalent governing body; or
- any involvement, other than through voting of shares, in substantive decisionmaking of the U.S. business regarding—
    - the use, development, acquisition, safekeeping, or release of sensitive personal data of U.S. citizens maintained or collected by the U.S. business;
    - the use, development, acquisition, or release of critical technologies; or
    - the management, operation, manufacture, or supply of critical infrastructure.

This new authority only applies to a non-controlling investment in a U.S. business that:

- produces, designs, tests, manufactures, fabricates, or develops one or more ***critical***
- ***technologies***;
- owns, operates, manufactures, supplies, or services ***critical infrastructure***; or
- maintains or collects ***sensitive personal data*** of U.S. citizens that may be exploited in a manner that threatens national security.

Treasury added that "FIRRMA also requires that CFIUS prescribe regulations that further define the term "foreign person" in the context of non-controlling investments by specifying criteria to limit its applicability over certain categories of foreign persons."

- Treasury highlighted "**Key Aspects of the Proposed Regulations Regarding "Covered Investments:"**
  Types of investments covered: Non-controlling investments that afford a foreign person certain
- access, rights, or involvement in certain U.S. businesses (referred to as "covered investments").
- **Largely a voluntary process:** Process remains largely voluntary, where parties may file a notice or submit a short-form declaration notifying CFIUS of a covered investment in order to receive a potential "safe harbor" letter (after which CFIUS does not initiate a review of a transaction except in certain limited circumstances). In some circumstances, filing a declaration for a transaction is mandatory. In particular, FIRRMA creates a mandatory declaration requirement for specified covered transactions where a foreign government has a "substantial interest". Additionally, FIRRMA authorizes CFIUS to mandate declarations for

covered transactions involving certain U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies.

- **U.S. businesses covered:** The new provisions on covered investments only apply to investments in U.S. businesses involved in specified ways with critical technologies, critical infrastructure, or
- sensitive personal data—referred to as "TID U.S. businesses" for ***t***echnology, ***i***nfrastructure, and ***d***ata.
    - **Critical technologies:** CFIUS may review transactions related to U.S. businesses that design, test, manufacture, fabricate, or develop one or more critical technologies. "Critical technologies" is defined to include certain items subject to export controls and other existing regulatory schemes, as well as emerging and foundational technologies controlled pursuant to the Export Control Reform Act of 2018.
    - **Critical infrastructure:** CFIUS may review transactions related to U.S. businesses that perform specified functions—owning, operating, manufacturing, supplying, or servicing—with respect to critical infrastructure across subsectors such as telecommunications, utilities, energy, and transportation, each as identified in an appendix to the proposed regulations.
    - **Sensitive personal data:** CFIUS may review transactions related to U.S. businesses that maintain or collect sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security. "Sensitive personal data" is defined to include ten categories of data maintained or collected by U.S. businesses that (i) target or tailor products or services to sensitive populations, including U.S. military members and employees of federal agencies involved in national security, (ii) collect or maintain such data on at least one million individuals, or (iii) have a demonstrated business objective to maintain or collect such data on greater than one million individuals and such data is an integrated part of the U.S. business's primary products or services. The categories of data include types of financial, geolocation, and health data, among others. Genetic information is also included in the definition regardless of whether it meets (i), (ii), or (iii).

Further Reading

- "Secret Service Investigates Breach at U.S. Govt IT Contractor" – *Krebs on Security*. A federal contractor was apparently breached as access to several of its systems was put up for sale on cybercrime site. This contractor works with a number of federal agencies. The Secret Service is investigating.
- "White House weighs controversial plan on mental illness and mass shootings" – *The Washington Post*. A friend of President Donald Trump's proposed the formation of a new agency along the lines of DARPA to use technological means to looks for signs that people may be tipping towards violent behavior. This is supposedly being serious consideration by the White House and Administration.
- "I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution." – *The New York Times*. The National Security Agency's General Counsel makes his case for the U.S. to shift its approach to technology and national security issues as we rune the risk of Losing the "digital revolution."
- "Real-Time Surveillance Will Test the British Tolerance for Cameras" – *The New York Times*. As more advanced cameras have come into use that utilize facial recognition technology, it remains unclear whether the people of the most domestically surveilled nation in the West will go along.

- "Ex-Google worker fears 'killer robots' could cause mass atrocities" – *The Guardian*. An engineer who left Google over its artificial project with the Department of Defense is claiming that the use of remote-controlled robots in combat could lead to "possible atrocities and unlawful killings even under laws of warfare, especially if hundreds or thousands of these machines are deployed."
- "U.S. got key asset out of Russia following election hacking" – *The Washington Post*. Like peeling an onion, the story of how Russia hacked and interfered with the U.S.'s 2016 election continues to yield more and layers. A Russian asset who provided intelligence about the 2016 hacking was exfiltrated in 2017 not long after President Donald Trump provided the Russian Foreign Minister with classified information in the Oval Office. Yet, the Central Intelligence Agency is claiming the two events are not related.
- "In 2011, Jeffrey Epstein Was A Known Sex Offender. The Leaders Of Amazon, Google, And Tesla Dined With Him Anyway." – *BuzzFeed News*. Turns out that leading tech figures attended a dinner with Jeffrey Epstein after he pled guilty to soliciting a girl for prostitution.
- "Huawei drops lawsuit against U.S. over seized equipment: court filing" – *Reuters*. The Chinese tech giant dropped its lawsuit against the U.S. arising from the seizure of equipment alleged to be in violation of U.S. export controls. Apparently, the U.S. returned the equipment in August and declined to file charges.
- "T-Mobile Has a Secret Setting to Protect Your Account From Hackers That It Refuses to Talk About" – *Motherboard*. What happens in Fight Club stays in Fight Club apparently. A little-known T-Mobile program requires customers to come into stores and present photo ID in order to get a new SIM card to fight SIM swapping.
- "Washington, Silicon Valley Struggle to Unify on Protecting Elections" – *Wall Street Journal*. A recent meeting in Silicon Valley between intelligence officials and tech officials resulted in Administration officials disagreeing on what role the technology industry should play in election security.
- "China responsible for Parliament House hacking, Australian intelligence agencies believe" – *The Canberra Times*. The Australian Signals Directorate determined that China's Ministry of State Security attacked Australia's Parliament and hacked into both parties. However, Australia is not going to make these accusations formally, for China is Australia's biggest trade partner.