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

Privacy Bill A Week: Consumer Online Privacy Rights Act

The last bill we examined on privacy and data security was Representatives Anna Eshoo (D-CA) and Zoe Lofgren's (D-CA) the "Online Privacy Act of 2019" (H.R. 4978), a long, comprehensive bill that has little chance of being enacted as it is. Another such bill has been introduced by Senate Democratic stakeholders that takes a comprehensive approach by marrying privacy and data security requirements. Senate Commerce Committee Ranking Member Maria Cantwell (D-WA) and three other Democrats on the committee, Brian Schatz (D-HI), Ed Markey (D-MA) and Amy Klobuchar (D-MN), have released the "Consumer Online Privacy Rights Act" (COPRA). This bill would empower the Federal Trade Commission (FTC) to police privacy and data security violations through augmented authority, not preempt state laws to the extent they provide greater protection, largely leave in place existing federal privacy statutes such as the "Financial Services Modernization Act of 1999" (aka Gramm-Leach-Bliley) and "Health Insurance Portability and Availability Act of 1996" (HIPAA), and allow individuals to sue. Of course, many of these approaches are contrary to the publicly espoused positions of numerous Republican and industry stakeholders. The sponsors released a one-page summary and a short report titled "The State of Online Privacy and Data Security."

COPRA was released ahead of the Senate Commerce, Science, and Transportation Committee's December 4 hearing "Examining Legislative Proposals to Protect Consumer Data Privacy," suggesting that Democrats wanted to define their positions on privacy and data security issues while also highlighting that the majority party in the Senate has failed to release a bill. It is unclear, however, if this bill signals that Cantwell's ongoing talks with Chair Roger Wicker (R-MS) have stalled. Cantwell and Wicker have been in discussions since the summer on a privacy bill after it appear the efforts undertaken by an ad hoc committee working group had not produced fruit. Nonetheless, Wicker stated that "[t]he legislation released today reflects where the Democrats want to go..[b]ut any privacy bill will need bipartisan support to become law." He added that "I am committed to continuing to work with the ranking member and my colleagues on both sides of the aisle to get a bill that can get across the finish line…[and] I expect that we will have a bill to discuss at next week's hearing."

It merits mention that Senator Richard Blumenthal (D-CT), the ranking member of the Manufacturing, Trade, and Consumer Protection Subcommittee, is not a cosponsor. Blumenthal has long called for both privacy and data security legislation and has often pressed federal agencies to better protect consumers. He has been working with the chair of the subcommittee, Senator Jerry Moran (R-KS), on a privacy bill, and yet despite having worked for over a year on a bill, no text has been released.

It also bears mention that the sponsorship of COPRA suggests that Senate Democrats are coalescing around a single position whereas its Members have taken a number of different approaches. The bill came shortly after Cantwell, and the top Democrats on three other committees released their principles for privacy legislation, signaling agreement on the broad outlines of such legislation. The other three ranking members were Patty Murray (D-WA) (Senate HELP), Dianne Feinstein (D-CA) (Senate Judiciary), and Sherrod Brown (D-OH) (Senate Banking). This agreement on principles

brokered by Senate Minority Leader Chuck Schumer (D-NY) may smooth some of the jurisdictional battles that have traditionally dogged attempts to address data security or cybersecurity.

Schatz, the ranking member on the Communications, Technology, Innovation and the Internet Subcommittee, led the drafting and introduction of the "Data Care Act," (S. 3744) in the last Congress. This bill which would extend the concept of fiduciary responsibility currently binding on health care professionals and attorneys with respect to the patients and clients' information to "online service providers" such as Facebook, Google, Apple, etc. (*See here* for more extensive analysis.) Likewise, Senator Ed Markey (D-MA) introduced the "Privacy Bill of Rights Act" (S. 1214), which was the only bill to get an A in the first draft of the Electronic Privacy Information Center's report on privacy bills. (*See here* for more analysis.) Finally, Klobuchar had cosponsored the "Data Care Act" and had also released a narrower bill with a Republican cosponsor, the "Social Media Privacy Protection and Consumer Rights Act of 2019" (S. 189), that would require major tech companies to give consumers an opportunity to opt in or opt out of the company's data usage practices after offering enhanced notice of the practices for which the personal data may used. (*See here* for more analysis.)

Under COPRA, entities covered by the new requirements is a broad class simply defined as those already subject to the FTC Act and "process[] or transfer[] covered data." The bill carves out sub-classes of entities that might otherwise be covered but some of which may not fall into the definition of covered entity.

Service providers are defined to be covered entities that are performing a service on behalf of another covered entity that process of transfer covered data. However, the definition is written to include only those activities undertaken at the behest of another covered entity and is explicit that the "term does not include a covered entity that processes or transfers the covered data outside of the direct relationship between the service provider and the covered entity." Consequently, entities such as Verizon and Amazon would be deemed service providers only to the extent they are providing services like broadband internet and cloud services. Otherwise, they would be covered entities and subject to all the responsibilities the bill would place on them. Third parties are those who received covered data from covered entities for processing or transfer that are not service providers, affiliates, subsidiaries, or otherwise controlled by the covered entity.

Additionally, small businesses would be carved out of much of the bill, and these are defined as those with $25 million or less in annual revenues for the preceding three years, processed the covered data of fewer than 100,000 individuals, and earns 50% or less of its gross revenue from processing covered data. So, non-profits and other discrete classes of entities would be outside the confines of this bill (e.g. some of the activities in the privacy and data security spheres of telecommunications companies would still be regulated by the Federal Communications Commission.)

"Covered data" is "information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data." But this term excludes "de-identified data," "employee data," and "public records." Turning to those terms, de-identified data are generally "information that cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household." However, before any such information may be deemed de-identified data, in addition to ensuring the information cannot be linked to a person, device, or household and also that inferences cannot be reasonably drawn, the entity must put in place reasonable measures to block the re-identification of such information and publicly commit not to re-identifying and to only process or transfer in a de-identified state.

Moreover, any entity seeking to de-identify data must also obligate any other entities who receive the information to meet all of the aforementioned requirements.

Employee data are the information employers collect, process, and transfer solely related to a person's employment, application for employment, emergency contacts, and administration of benefits. Public records are "information that is lawfully made available from Federal, State, or local government records provided that the covered entity processes and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity." This last definition may receive some scrutiny, for a number of Departments of Motor Vehicles are selling the personal information of people who hold driver's licenses, so this could prove a significant loophole that may be exploited.

COPRA creates a subset of covered data, "sensitive covered data," which includes the following list, which has been shortened:

- A government-issued identifier, such as a Social Security number, passport number, or driver's license number.
- Any information that describes or reveals the past, present, or future physical health, mental health, disability, or diagnosis of an individual.
- Biometric information.
- Precise geolocation information that reveals the past or present actual physical location of an individual or device.
- The content or metadata of an individual's private communications or the identity of the parties to such communications unless the covered entity is an intended recipient of the communication.
- Information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information.
- Information revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information.
- Information revealing online activities over time and across third-party website or online services.
- Calendar information, address book information, phone or text logs, photos, or videos maintained on an individual's device.
- A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.
- Any other covered data processed or transferred for the purpose of identifying the above data types.
- Any other covered data that the Commission determines to be sensitive covered data through a rulemaking pursuant to [the Administrative Procedure Act]

While we will not dive into all the categories of information considered sensitive covered data, one bears mention for it sets COPRA apart from the only major privacy bill introduced in the House this year, the "Online Privacy Act of 2019" (H.R. 4978). In COPRA, both the content and metadata of private communications are provided privileged status. The same is not true in the other bill, which protects only the contents of communications with metadata being subject to lesser standards.

A final definition to note: "affirmative express consent." Since so much of a person's rights under COPRA is linked to the provision of "affirmative express consent," it bears a bit of investigation.

First, the bill makes clear that this cannot be inferred by a person's actions or inaction or even her continued use of a covered entity's products and services. Consequently, only affirmative actions that clearly communicate agreement in response to a specific request that meets defined criteria will qualify. Namely, this request must be by itself, describe each act or practice for which consent is being requested, expressed in easily understood language, and explains applicable rights. Any consent short of this would violate the Act, for then any subsequent processing or transference of covered data would be contrary to a number of requirements.

Covered entities would have a duty of loyalty. However, the bill is not explicit as to whom this duty if owed, but the context is fairly clear that this duty is due to the people whose covered data is collected, processed, and transferred. This duty has two parts: 1) a prohibition against engaging in deceptive or harmful data practices; and 2) processing or transferring covered data in any way that violates COPRA. The definition of what is deceptive is the same as those practices currently barred as deceptive under the FTC Act, but COPRA would institute a new definition of harmful that would considerably widen the scope of the FTC's powers to punish illegal privacy or data security practices. Specifically, harmful data practices are "the processing or transfer of covered data in a manner that causes or is likely to cause any of the following:

- Financial, physical, or reputational injury to an individual.
- Physical or other offensive intrusion upon the solitude or seclusion of an individual or the individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person.
- Other substantial injury to an individual."

Obviously, the FTC will have views on how to construe some potentially harmful data practices that will ultimately be adjudicated upon by federal courts. For example, how would one define "reputational harm"? Likewise, what constitutes "[o]ther substantial injury" given that financial, physical, reputational, and broad privacy harms are already enumerated. Quite possibly, this language was included to provide the agency and courts with the flexibility to include new harms yet to be seen. As for the other component of the duty of loyalty, it is simply not to violate the myriad requirements of the Act, which provides a very broad means for the FTC and state attorneys general to pursue and prosecute violations.

People would be able to request and receive a human-readable version of their covered data a covered entity holds along with the names of all third parties with whom such information has been shared and why. Covered entities must make publicly available "a privacy policy that provides a detailed and accurate representation of the entity's data processing and data transfer activities." This policy must include

- each category of data the covered entity collects and the processing purposes for which such data is collected
- whether the covered entity transfers covered data and, if so—
    - each category of service provider and third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such categories; and
    - the identity of each third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such third party, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such transfer;
- how long covered data processed by the covered entity will be retained by the covered entity and a description of the covered entity's data minimization policies;

- how individuals can exercise his or her individual rights; and
- a description of the covered entity's data security policies

This is a fairly comprehensive list of information a consumer must be provided. Unless the FTC issues regulations or guidance directing covered entities to use a uniform format or keep this disclosure to a certain length, it is possible covered entities will favor longer, denser privacy policies in order to either obfuscate or discourage reading.

And, of course, any material changes to a covered entity's privacy policy will require obtaining affirmative express consent from users.

Another right granted by COPRA is that of deletion. Upon receiving a verified request from a person, a covered entity must delete the requested information and then also inform third parties and service providers of the deletion request. However, it is not clear that the latter two entities would be bound to honor the request and actually carry out the deletion. It may be necessary for the FTC"s regulations to require such language be inserted into contracts between covered entities and their service providers and third parties.

Likewise, an individual may ask that a covered entity correct any inaccuracies in the covered data they hold and process. Again, any such request would need to be verified and again the covered entity would need to inform third parties and service providers.

The bill creates a right of data portability in that covered entities must honor verified requests from people and provide them with both human-readable and machine-readable copies of their covered data. COPRA also establishes a right to object to and opt-out of transfers of covered data to third parties, and the FTC would need to conduct a rulemaking to establish the procedures one may use to affect this right. The bill lists the features this final rule must have, including requirements for clear and conspicuous opt-out notices and easy to use mechanisms and a centralization of opting out so a person will not need to repeatedly opt-out of a covered entity's transfers.

Furthermore, covered entities may neither process nor transfer a person's sensitive covered data with "prior, affirmative express consent" and must "provide an individual with a consumer-friendly means to withdraw affirmative express consent to process the sensitive covered data of the individual." However, covered entities do not need prior, affirmative express consent to process or transfer publicly available information. Considering that these passages are in the same section of the bill, the drafters are clearly contemplating that sensitive covered data may be available from public sources. For example, as mentioned earlier, some DMVs are selling the personal information of drivers, making some available information that would likely be considered sensitive covered data that could then be processed and transferred without the consent of the person to which it pertains.

Covered entities must limit their data processing and transferring to what is necessary, proportionate, and limited. This right to data minimization would task covered entities with engaging in the bare minimum "to carry out the specific processing purposes and transfers described in the privacy policy made available by the covered entity as required" unless it has affirmative express consent for other processing or transferring. This right to data minimization would be abridged by the exceptions discussed below.

Cantwell has long expressed her view that privacy legislation should include data security requirements, and so COPRA does. Covered entities must "establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data…appropriate to the volume and nature of the covered data at issue." This provision spells out further requirements, including the need to conduct vulnerability assessments to turn up reasonable foreseeable threats, developing and implementing a process to address any such vulnerabilities, destroying or deleting any covered data that is no longer needed or for which affirmative express consent to hold has not been provided, and to properly train the covered entity's employees to properly handle and safeguard covered data. The FTC would need to issue training guidelines to assist covered entities, and even though this provision does not specifically task the agency with promulgating regulations, COPRA provides the FTC with a broad grant of authority to promulgate regulations under the Administrative Procedure Act.

Next, the bill turns to the civil rights granted to individuals residing in the U.S. regarding data privacy, many of which address practices the Obama Administration called digital redlining. Covered entities are barred from processing or transferring covered data on the basis of real, or perceived, classes, including but not limited to, race, national origin, ethnicity, gender, sexual orientation and others, for a variety of defined purposes. Broadly speaking the purposes for processing and transferring covered data using protected classes pertain to differentiating opportunities for employment, education, housing, and credit on the basis of different classes. As an example of a practice that would be barred is the Department of Housing and Urban Development's allegations that Facebook allowed people placing ads on the social platform to target certain racial groups and exclude others. This bar on discriminatory treatment would also be applied to public accommodations writ large meaning any services or products offered generally to the public. Consequently, covered data could not be used by covered entities to discriminate against women, for example, in providing a different, lower price for men for a service. Additionally, "[a] covered entity may request advice from the Commission concerning the covered entity's potential compliance with this subsection, in accordance with the Commission's rules of practice on advisory opinions."

These civil rights are extended to algorithmic decision making. Covered entities using algorithmic decision making in processing or transferring covered data in the same contexts must perform impact assessments annually, keep them on file, and make them available to the FTC upon request. Presumably, the FTC could use these impact assessments as evidence, if warranted, in finding that a covered entity has violated the Act through discriminatory actions flowing from such decision making. In any event, the FTC would be required to public a report "examining the use of algorithms" for decision making in this context within 3 years of enactment and then every 3 years thereafter.

COPRA would bar people from being allowed to waive certain of their rights under any circumstances and other rights under circumscribed circumstances. Those rights that cannot be waived are the duty of loyalty covered entities owe to people, data portability, data minimization, data security, and the various civil rights. And yet, the rights of access, transparency, deletion, correcting inaccuracies may be waived if three circumstances are present:

- "there exists a direct relationship between the individual and the covered entity initiated by the individual;
- the provision of the service or product requested by the individual requires the processing or transferring of the specific covered data of the individual and the covered data is strictly necessary to provide the service or product; and

- an individual provides affirmative express consent to such specific limitations."

Of course, in the latter category, covered entities that believe all three conditions are at work will prompt or perhaps even require people to waive those rights. And, it is all but certain that covered entities will seek to expand as much as possible the concept of what "is strictly necessary to provide the service or product." Consequently, should the provision of a service such as FaceTime require the processing and/or transfer of covered data, then Apple would need to obtain affirmative, express consent and only after an individual initiates the relationship. However, would covered entities be able to advertise or spam people with offers for their services and products in exchange for waivers? Also, it will undoubtedly be a point of contention as to what processing and transferring of covered data is necessary for certain services and products to be provided. Presumably, a company like Google could make the case that its provision of free email through Gmail is financed through the harvesting and sharing of data and without this, it is not viable. It seems to me the FTC will need to weigh in on the contours of what constitutes "strictly necessary" in terms of seeking waivers from these rights.

Of course, the exercise of a number of these rights hinges on verifying that the person making the request is who he claims to be (i.e. the rights to access, transparency, deletion, correction, and portability). Covered entities would be able to deny people the exercise of these rights if they cannot reasonably verify the identity of the requester, which seems on its face a reasonable step to avoid allowing people to make mischief with others' data and accounts. Covered entities must request additional information to verify a person's identity in cases of uncertainty. In any event, covered entities must minimize burdens and cannot charge for these requests.

And yet, there circumstances that would allow covered entities to deny these requests:

- if complying with the request would be demonstrably impossible,
- complying with the request would prevent the covered entity from carrying out internal audits, performing accounting functions, processing refunds, or fulfilling warranty claims, provided that the covered data that is the subject of the request is not processed or transferred for any purpose other than such specific activities;
- the request is made to correct or delete publicly available information, and then only to the extent the data is publicly available information;
- complying with the request would impair the publication of newsworthy information of legitimate public concern to the public by a covered entity, or the processing or transfer of information by a covered entity for such purpose;
- complying with the request would impair the privacy of another individual or the rights of another to exercise free speech; or
- the covered entity processes or will process the data subject to the request for a specific purpose described in [provisions detailing when express affirmative consent is not needed], and complying with the request would prevent the covered entity from using such data for such specific purpose

However, covered entities may also deny these requests if they reasonably believe they would interfere with a contract between the covered entity and another individual.

COPRA also stipulates that "[t]he rights and remedies provided for in this section shall not be waived by any policy form or condition of employment, including by a predispute arbitration agreement." Moreover, "[n]o predispute arbitration agreement shall be valid or enforceable if the agreement requires arbitration of a dispute."

As noted earlier, covered entities may process or transfer covered data without in the affirmative express consent of a person "provided that the processing or transfer is reasonably necessary, proportionate, and limited to such purpose:

- To complete a transaction or fulfill an order or service specifically requested by an individual, such as billing, shipping, or accounting.
- To perform system maintenance, debug systems, or repair errors to ensure the functionality of a product or service provided by the covered entity.
- To detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service.
- To protect against malicious, deceptive, fraudulent or illegal activity.
- To comply with a legal obligation or the establishment, exercise, or defense of legal claims.
- To prevent an individual from suffering harm where the covered entity believes in good faith that the individual is in danger of suffering death or serious physical injury.
- To effectuate a product recall pursuant to Federal or State law.
- To conduct scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or a similar oversight entity that meets standards promulgated by [the FTC in an APA rulemaking.]

The FTC and state attorneys general will need to closely monitor the use of these exceptions by covered entities, for the inclination of regulated entities is to push the limits of legal or excepted behavior. Consequently, regulators will need to review the use of these exceptions lest one or more become the exception that ate the federal privacy statute.

The FTC will need to promulgate regulations "identifying privacy protective requirements for the processing of biometric information" for two of the above exceptions to the requirement for affirmative express consent: to detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service, or to protect against malicious, deceptive, fraudulent or illegal activity. This section further details the requirements of such a rulemaking.

The bill carves out "the publication of newsworthy information of legitimate public concern to the public by a covered entity, or to the processing or transfer of information by a covered entity for that purpose."

COPRA would exempt those covered entities subject to other federal privacy and data security statutes such as the "Financial Services Modernization Act of 1999" (aka Gramm-Leach-Bliley) and "Health Insurance Portability and Availability Act of 1996" (HIPAA) to a certain degree. There are provisions making clear that entities in compliance with the named federal regimes shall be deemed to be in compliance with the privacy and data security requirements of COPRA "with respect to data subject to the requirements of such regulations, part, title, or Act." This would suggest that for data that falls outside those regimes (e.g. biometric data and geolocation data are not subject to Gramm-Leach-Bliley), any covered entities would need to meet the privacy and data security requirements of COPRA in addition to their existing responsibilities. The FTC must issue guidance describing the implementation of this section within one year.

COPRA would add compliance responsibilities for "large data holders," those covered entities that process or transfer the covered data of 5 million or more individuals per year or processed or

transferred the sensitive covered data of 100,000 or more individuals in a year. These entities would need to annually certify compliance with the Act after a review of its internal procedures and processes for compliance. The CEO, chief privacy officer, and chief data security officer must sign this certification. This language is obviously aimed at the largest of data collectors and processors and is intended to make the CEOs aware and responsible for privacy and data security practices, so they would not be able to claim they were ignorant of problems that turn up.

However, all covered entities must designate both chief privacy and chief data security officers who "shall be responsible for, at a minimum—

- implementing a comprehensive written data privacy program and data security program to safeguard the privacy and security of covered data throughout the life cycle of development and operational practices of the covered entity's products or services;
- annually conducting privacy and data security risk assessments, data hygiene, and other quality control practices; and
- facilitating the covered entity's ongoing compliance with this Act."

COPRA spells out the responsibilities of service providers and third parties. Service providers may only process covered data in accordance with the wishes of the covered entity from whom it received the information or to comply with a legal obligation. Service providers may not transfer covered data "without the affirmative express consent… of the individual to whom the service provider data is linked or reasonably linkable." Additionally, service providers must delete or de-identify covered data once they have completed their services for a covered entity. Third parties may not "process third party data for a purpose that is inconsistent with the expectations of a reasonable individual" and "may reasonably rely on representations made by the covered entity that transferred third party data regarding the expectation of a reasonable individual, provided the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible." Service providers and third parties would be exempted from some of the rights people would be given under COPRA (e.g. the right of access.)

Covered entities must exercise reasonable due diligence regarding service providers and third parties:

- in selecting a service provider and conduct reasonable oversight of its service providers to ensure compliance with the applicable requirements of this section; and
- in deciding to transfer covered data to a third party, and conduct oversight of third parties to which it transfers data to ensure compliance with the applicable requirements of this subsection.

The bill has provisions to protect and encourage whistleblowers in coming forward to uncover illegal privacy and data security practices. Additionally, the National Institute of Standards and Technology "shall publish a report regarding digital content forgeries," an area of increasing concern for policymakers as deep fakes become more and more prevalent and lifelike.

With respect to enforcement, the FTC would receive broad authority to draft regulations and guidance to effectuate COPRA. The FTC and state attorneys general could bring actions under this bill. They could seek civil penalties of $42,530 per violation in the first instance and all the other relief that can currently be sought such as equitable remedies including rescission, disgorgement, and injunctions. All of this is fairly anodyne and even Republicans have come to accept what they long resisted earlier in the decade when data security legislation was debated and opposed state attorneys general getting on the field or giving the FTC authority to seek fines for first offenses.

However, what many stakeholders may be relying on is that the FTC and state attorneys general are only capable of bringing so many actions and there may well be conduct that goes unpunished that is quite possibly at odds with COPRA.

Additionally, the FTC must "establish a new Bureau within the Commission comparable in structure, size, organization, and authority to the existing Bureaus with the Commission related to consumer protection and competition" within two years of enactment. However, this bill does not specifically authorize extra appropriations for this purpose and rather includes language authorizing those sums necessary to implement the Act. And, without additional funds to set up and resource this new Bureau, then this may be a hollow grant of authority that may be obeyed by the FTC cannibalizing its other current operations. However, an account titled the "Data Privacy and Security Relief Fund" would be established to collect all civil awards won by the FTC and to primarily make consumers whole who were harmed by covered entities.

As noted, individuals could sue for violations in any competent federal or state court and could win the greater of actual damages and between $100-$1000 per violation, punitive damages, and attorney's fees. This is the most expansive such right in a major privacy bill released this year and may be seen as the lynchpin of enforcement efforts, for if state attorneys general and the FTC are only able to police a small set of violations, then people and their attorneys through the use of class actions may be able to enforce the statute for many companies may emphasize compliance in order to avoid a huge settlement. And yet, giving plaintiffs' attorneys another means by which they can sue corporations is anathema to Republicans. Therefore, it will be an uphill battle for any private right of action to survive in a final privacy and data security bill passed by the Senate and sent to the White House.

CR Carries Short Term FISA Extension

Tucked into the month-long FY 2020 continuing resolution (CR) (H.R. 3055) extending government funding through December 20 was language extending provisions of the Foreign Intelligence Surveillance Act (FISA) set to expire on December 15, 2019. The three-month extension will allow the Intelligence Community to continue to use the following authorities: the 1) call detail records provisions; 2) roving wiretap authority; 3) the lone wolf provision; and the 4) business records provisions. These extensions kicks a contentious legislative issue into next year as none of the committees of jurisdiction have produced legislative proposals on how to reauthorize these programs. Moreover, ten House Democrats voted against the CR because of the FISA extension language, presaging what may prove a difficult process for longer-term extensions next year, including Representatives Rashida Tlaib (D-MI), Alexandria Ocasio-Cortez (D-NY), Ayanna Pressley (D-MA), and Ilhan Omar (D-MN).

The Trump Administration asked that Congress permanently extend these programs instead of reauthorizing them for a period of years as has been the custom since passage of the USA Patriot Act in 2001. In an August letter sent before he stepped down, former Director of National Intelligence Dan Coats asked the Senate and House Intelligence and Judiciary Committees for "the permanent reauthorization of the provisions of the USA FREEDOM Act of 2015 that are currently set to expire in December…[that] provide the IC with key national security authorities." However, a number of Democratic stakeholders have balked at a permanent reauthorization of these programs, especially the call detail records program because the national Security Agency (NSA) has shut down the program. Nonetheless, the Administration is requesting those authorities in the event there is a need in the future.

Senate Passed Cyber Legislation

The Senate passed two-narrowly focused cybersecurity measures, sending them to the House. The first bill, the "National Cybersecurity Preparedness Consortium Act of 2019" (S. 333), was passed without amendment. This legislation would allow the Department of Homeland Security (DHS) to "work with a consortium to support efforts to address cybersecurity risks and incidents." A consortium is defined to be "a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security." DHS could direct the National Cybersecurity & Communications Integration Center (NCCIC) to work with a consortium to provide a range of services or achieve a number of goals, including help train first responders to respond to and recover from cyber incidents; provide technical expertise; and conduct cross-sector cybersecurity training and simulation exercises. A House companion bill, H.R. 1062, has not been acted upon.

A few key things to mention about this targeted cyber bill. First, the definition of what constitutes a consortium seems to leave wriggle room for private sector participation: "a group primarily composed of nonprofit entities, including academic institutions, that develop, update, and deliver cybersecurity training in support of homeland security." Because of the way this is written, there would seem to be a place for private sector entities in a consortium so long as it is "primarily composed" of nonprofit entities.

Also, DHS may utilize these consortia but is under no obligation to do so. The grant of authority is entirely discretionary. That being said, DHS would likely have a hard time explaining to Congress why it is not using existing expertise particularly given what every stakeholder agrees is a dearth of cyber talent in federal, state, and local governments. Moreover, these consortia would presumably increase the pipeline of university cyber talent to the state and local governments and private sector.

S. 333 is sponsored by Senators John Cornyn (R-TX), Pat Leahy (D-VT), Ted Cruz (R-TX) and John Boozman (R-AR) and reflects the existence of entities that might stand to take advantage of such a program. The National Cybersecurity Preparedness Consortium consists of five universities, including the University of Texas at San Antonio's (UTSA) Center for Infrastructure Assurance and Security (CIAS) and the Texas A&M Engineering Extension Service (TEEX) National Emergency Response and Recovery Training Center (NERRTC). The Norwich University Applied Research Institutes (NUARI) is in Vermont, the Cyberterrorism Defense Initiative (CDI) in Arkansas, and the University of Memphis Center for Information Assurance (CfIA) in Tennessee. Another entity that possibly qualify is the Cyber & Information Security Consortium, LLC (CISC), which consists of "the Oak Ridge National Laboratory and the University of Tennessee, – have joined with Cisco Systems, CNS, Sword & Shield Enterprise Security, the East Tennessee Economic Council and other private corporations."

The other bill, the "State and Local Government Cybersecurity Act of 2019," (S. 1846) was changed before passage. The amendment struck language on a pilot to deploy sensors unrelated to the main purpose of the legislation. DHS would be authorized "[t]o make grants to and enter into cooperative agreements or contracts with States, local, Tribal, and territorial governments, and other non-Federal…to carry out the responsibilities of the Secretary related to cybersecurity and infrastructure…including grants, cooperative agreements, and contracts that provide assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings." Entities eligible to participate include:

- an association, corporation, whether for-profit or nonprofit, partnership, proprietorship, organization, institution, establishment, or individual, whether domestic or foreign;
- a governmental agency or other governmental entity, whether domestic or foreign, including State, local, Tribal, and territorial government entities; and
- the general public.

NCCIC would also be tasked with new, related responsibilities and must "to the extent practicable, and in coordination as appropriate with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center:

- conduct exercises with Federal and non-Federal entities;
- provide operational and technical cybersecurity training related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents to Federal and non-Federal entities to address cybersecurity risks or incidents, with or without reimbursement;
- assist Federal and non-Federal entities, upon request, in sharing cyber threat indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government as well as among Federal and non-Federal entities, in order to increase situational awareness and help prevent incidents; and
- provide notifications containing specific incident and malware information that may affect them or their customers and residents.

House Energy and Commerce Marks Up and Reports Out Tech Bills

On November 19, the House Energy and Commerce Committee marked up a number of technology and 5G related bills:

- The "Broadband Deployment Accuracy and Technological Availability Act" (H.R. 4229) as amended. In a memorandum, the committee explained that H.R. 4779 "would require the Federal Communications Commission (FCC) to issue new rules to require the collection and dissemination of granular broadband availability data. It would also require the FCC to establish a process to verify the accuracy of such data, including by using data submitted by other government entities or the public. In addition, the bill would require the FCC to use this data to create coverage maps based on a serviceable location fabric map regarding fixed broadband."
- The "Mapping Accuracy Promotes Services (MAPS) Act" (H.R. 4227) that "specifies that it is unlawful for a person to willfully, knowingly, or recklessly submit broadband service data that is inaccurate."
- The "Studying How to Harness Airwave Resources Efficiently (SHARE) Act of 2019" (H.R. 5000) that "would require the National Telecommunications and Information Administration (NTIA), in consultation with the FCC, to establish a spectrum sharing and prototyping program and test bed to explore new ways for federal entities to share spectrum with other federal entities." Staff added that "[t]he legislation would authorize $50 million for NTIA to establish the spectrum sharing prototyping and test bed program…[and] would also require NTIA and the FCC, in consultation with the National Institute of Standards and Technology, to submit a report to Congress on how to improve and expand the spectrum sharing techniques developed for the 3.5 GHz band, or other spectrum sharing strategies, and consider their applicability to other bands, including 3.1 GHz to 3.55 GHz and 7.1 GHz to 8.4 GHz, among other considerations."
- The "Secure and Trusted Communications Networks Act of 2019" (H.R. 4998) would direct "the FCC to develop and maintain a list of communications equipment and services that pose an unacceptable risk to national security and prohibits the use of funds made available by

FCC programs to purchase, rent, lease, or otherwise obtain such equipment and services…[and] also establishes the Secure and Trusted Communications Reimbursement Program to assist communications providers with the costs of removing prohibited equipment and services from their networks and replacing prohibited equipment with more secure communications equipment and services."

- The "Network Security Information Sharing Act of 2019" (H.R. 4461) "directs the Secretary of Homeland Security, in cooperation with the Director of National Intelligence (DNI), the Director of the Federal Bureau of Investigation, NTIA, and the FCC, to establish a program to share supply chain security risks with advanced communications service providers and trusted suppliers of telecommunications equipment and services." The bill was reported without amendment by voice vote.
- The "Secure 5G and Beyond Act of 2019" (H.R. 2881) "directs the President to develop the "Secure Next Generation Mobile Communications Strategy" in consultation with the heads of the FCC, NTIA, and Department of Homeland Security, as well as the DNI and Secretary of Defense." Staff explained that "[t]he Secure Next Generation Mobile Communications Strategy is intended to: (1) ensure the security of 5G communications systems and infrastructure in the United States; (2) assist mutual defense allies and strategic partners in maximizing the security of 5G networks and infrastructure in their countries; and (3) protect the competitiveness of U.S. companies, the privacy of American consumers, and the integrity of standards-setting bodies against political influence." The bill was reported without amendment by voice vote.
- The "Promoting United States Wireless Leadership Act of 2019" (H.R. 4500) "directs NTIA to encourage participation by trusted American companies and other stakeholders in standards-setting bodies, and to offer technical assistance to such stakeholders that elect to participate, in the course of developing standards for 5G networks and future generations of communications networks."
- H.Res. 575 that "expresses the sense of the House of Representatives that stakeholders involved in the deployment of 5G communications infrastructure should consider adherence to the international security recommendations adopted at the Prague 5G Security Conference in May 2019, known as "The Prague Proposals"…[and] also encourages the President and federal agencies to promote trade and security policies on the international stage that are consistent with "The Prague Proposals."
- An extension of the "Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders US SAFEWEB) Act of 2006" (H.R. 4779) authorities enacted in 2006 "to improve the FTC's ability to combat unfair or deceptive acts or practices that are international in scope."

Senate Democrats' Privacy Principles

The Ranking Members on four Senate Committees of jurisdiction over privacy and data security issues have released the principles they want to see present in any such legislation. Not surprisingly, there are a number of principles that are not going to be readily or easily accepted by Republicans and many industry stakeholders. For example, the principles do not call for a national statute that would preempt state laws like the "California Consumer Privacy Act" (AB 375), which is considered by many stakeholders a crucial part of any bill implementing federal privacy requirements. Additionally, Senate Democrats would favor a private right of action for people against companies for alleged violations. Again, this is contrary to the oft-repeated position of Republicans.

Nonetheless, Senators Maria Cantwell (D-WA), Dianne Feinstein (D-CA), Patty Murray (D-WA), and

Sherrod Brown (D-OH) agreed to these principles, and reportedly Senate Minority Leader Chuck Schumer (D-NY) convened and facilitated the effort, which has come ahead of the release of the privacy bills that have been under development this year in the Senate. Of course, the Senate Commerce, Science, and Transportation Committee had convened an informal working group late last year consisting of Cantwell, Chair Roger Wicker (R-MS) and Senators John Thune (R-SD), Jerry Moran (R-KS), Brian Schatz (D-HI), and Richard Blumenthal (D-CT) to hash out a privacy bill.

However, like most other such efforts, the timeline for releasing bill text has been repeatedly pushed back even after Wicker and Cantwell tried working by themselves on a bill late in the summer. Additionally, Moran and Blumenthal, the chair and ranking member of the Manufacturing, Trade, and Consumer Protection Subcommittee, have been working on a bill for some time as well but without a timeline for releasing text. And, the efforts at this committee are in parallel to those in other committees. Senate Judiciary Chair Lindsey Graham (R-SC) has gotten his committee onto the field with hearings on the subject and has articulated his aim to play a role in crafting a bill. Likewise, the Senate Banking Committee has held hearings and are looking to participate in the process as well. But, like Senate Commerce, no bills have been released.

In terms of the substance of the principles, the four ranking members stated that this "set of core principles...should be included in any comprehensive data protection legislation." They claimed that "[u]nder our framework, consumers would control their personal information, and corporations, non-profits, and political entities would be held to higher standards for when and how they collect, use, share, and protect our data." The ranking members cautioned that "[n]othing in this framework should be interpreted to change or displace existing privacy laws, or privacy laws scheduled to go into effect" (e.g. the CCPA or existing federal privacy statutes and regulations like the Children's Online Privacy Protection Act (P.L. 105-277) or the "Health Insurance Portability and Accountability Act of 1996" (P.L. 104-101)).

As a general matter, drafting principles is, of course, easier than drafting legislation, and it gives stakeholders less to take issue with. Nonetheless, in our analysis we wanted to touch the points at which Senate Republicans and industry stakeholders may not agree with the ranking members.

ESTABLISH DATA SAFEGUARDS

- **Minimization:** Collection of data must be minimized so that it is narrowly tailored to its authorized use. We must establish strict limits around the use, extrapolation, and retention of certain data, especially data relating to biometrics, race, sexual orientation, children, health, or finances.
- **Abuse Prevention:** Harmful, deceptive, and abusive collection and use of data must be prohibited. Standards must ensure that data is only processed in a transparent manner that meets consumers' expectations and is free from unlawful manipulation.
- **Sharing Limits:** To ensure that consumers are protected throughout the marketplace, we must establish clear rules to limit data sharing with service providers and third parties to that which is needed to carry out the express purposes expected and authorized by consumers.
- **Security:** We must provide greater accountability and higher standards over the way organizations retain and secure data.

In this section, the language that might get flagged by Republicans includes the call to minimize data collection for many stakeholders see great value in using data in new ways and repurposing data. Some stakeholders would likely insist that economic progress in the technology sector would

depend on experimenting with new uses for data. And, of course, the appropriate degree of tailoring data usage will differ depending on one's perspective. Additionally, while limits on harmful and abusive uses of data are acceptable to everyone, defining what constitutes abuse and harm is where divides will form, especially since Democrats are calling for an end to "unlawful manipulation" suggesting they will want to make certain types of data processing off limits. Republicans have generally been more comfortable with giving companies flexibility so long as consumers are clearly and transparently informed and consent to such uses. The language on sharing limits seems to suggest that some practices may be deemed off limits, but then the clause on predicating sharing on express consent pushes this principle back towards to enhanced notice and consent model. There is a great deal of agreement that so long as consumers are informed in an easy to understand fashion, they should be allowed to let entities use their personal data. Finally, regarding data security, a number of high-profile Democrats have insisted that data security is a sine non qua of privacy legislation, including Cantwell, so it is not a surprise this language made it into a statement of principles. It has been remarkable the extent to which Republicans have been willing to let go of their opposition to pairing data security with privacy.

INVIGORATE COMPETITION

- **Market Power Checks:** Consumers must have the ability to prevent their data from being commingled across separate businesses within an enterprise, and to ensure that privacy protections, including restrictions on commingling or repurposing, apply to data obtained through mergers, acquisitions, or bankruptcies.
- **Data Portability:** To boost choice in the marketplace and level the playing field for entrepreneurs, consumers must be empowered to take their data to the company of their preference.

Barring a company from sharing data across its subsidiaries sounds like a non-starter with many stakeholders, and regarding data portability, the fight will be over the details, naturally. On this latter point, almost all the Democratic bills introduced this year have included language requiring covered entities to provide people with their data upon making a verified request so they may use it presumably with another entity. Industry stakeholders are going to have a hard case to make that people being able to leave a platform like Twitter for a competitor is a bad thing for competition, and in light of myriad antitrust investigations, large technology companies will have to delicately finesse public opposition to such provisions.

STRENGTHEN CONSUMER AND CIVIL RIGHTS

- **Individual Consumer Rights:** Consumers must have the right to control their data, including the right to know, access, delete, correct, and restrict the transfer and retention of their records. Organizations that collect and store our data must be required to provide clear, concise disclosure of and justification for their privacy practices, and supply consumers with meaningful options to access products or services without sacrificing their privacy. We must also have heightened protections and tools in place, like a do-not-track right, to prevent consumers from being targeted online and tracked across websites, and to protect children and teens.
- **Civil Rights Protections:** Computer-based decisions that result in illegal bias or discrimination are unacceptable. Consumers must have transparency into black box algorithmic decisions that may result in bias or discrimination, and the ability to challenge such decisions. Entities that process consumer data in automated systems must be required to review such algorithms in order to prevent discriminatory impact. Enforcers must also be

fully equipped to protect against unlawful discrimination in addition to voter targeting and suppression.

Again, the details will matter here because a number of these principles coincide with generally held Republican notions of what privacy legislation should address. However, the notion that people should be able to access services and products without agreeing to data practices is a likely non-starter as is a do-not-track right. It bears note that many of the Democratic bills generally bar forcing people to waive their privacy rights in exchange for services or products unless it is not possible for such service or product to be provided without the data in question. I think it is quite likely that such language makes it into a final privacy bill, meaning industry will likely make the case to interpret necessity as widely as possible. Discrimination on the basis of automated decision-making is a new frontier legislatively, and it's unclear how this is addressed, if at all, in legislation. However, on its face, the notion that artificial intelligence will be making decisions with serious consequences would likely give most lawmakers pause. And yet, the front may form over whether it is necessary to prove a discriminatory intent in algorithmic decision making as opposed to a discriminatory impact arising from what seems the use of neutral decision making. Finally, given the opposition of many Republicans, most notably Senate Majority Leader Mitch McConnell (R-KY), on legislation delving into election issues, it is likely any such language on the practices for targeting voters encouraging or discouraging them to vote would not make it into a final bill.

IMPOSE REAL ACCOUNTABILITY

- **Corporate Accountability:** Accountability mechanisms must shift the responsibility and liability of protecting privacy from consumers, who are overly burdened with understanding complicated, take-it-or-leave-it privacy policies, to the entities that hold their data and their senior corporate executives. Consumers must be able to trust that organizations secure their data, use it ethically, and do not use it to consumers' detriment. Increased Chief Executive Officer (CEO) accountability, whistleblower rights, and consumer redress mechanisms are just a few of the many tools that must be provided to ensure corporations are held to account.
- **Federal Enforcement and Rulemaking:** Enforcement of privacy rights must serve as a serious deterrent, not just an acceptable cost of doing business. Among other changes, federal enforcers must be able to seek significant civil fines and criminal penalties, where possible, in the first instance of privacy and data security violations. Federal enforcers must also have streamlined rulemaking authority to ensure that the strong legal protections imposed by this law can evolve and adapt to new technologies, and equipped with adequate staff and resources to implement these protections.
- **State and Private Remedies:** Federal enforcement must be complemented by state enforcement of federal protections and private rights of action, as is common in existing privacy laws and other fields. The private right of action must be meaningful, and not one that can be overridden by a mandatory arbitration clause buried within onerous and lengthy terms and conditions.

Much of the language on corporate accountability may prove unacceptable to stakeholders, notably the notion of increased CEO accountability. Do the ranking members mean criminal liability? Financial liability? It is not possible to tell from this brief passage. Also, the language here seems at odds with the principle of an enhanced notice and consent regime detailed elsewhere in the principles. However, Senate Democrats may envision a regime where certain practices or either off limit or the responsibility of the entities using a consumer's data with room for people to consent, or not, to certain acceptable data uses after being properly informed. Regarding enforcement and

rulemaking, the ranking members are basically calling for the FTC to be the primary privacy regulator since they are calling for civil fine enforcement authority for first offenses and for streamlined rulemaking authority. Currently the FTC cannot levy fines for first offenses and has a cumbersome rulemaking process. It bears note that the Senators opted against the approach proposed by Representative Eshoo (D-CA) and Lofgren (D-CA) in their "Online Privacy Act of 2019" (H.R. 4978) who decided to bypass the FTC and establish a new agency. However, they are also calling for criminal penalties, which likely means adding criminal violations to the federal criminal code that would allow the U.S. Department of Justice to criminally prosecute offenders. Consequently, the previous passage on corporate responsibility that suggested criminal liability would, indeed, mean top corporate officials facing criminal fines and convictions in order to ensure compliance. Finally, a private right of action is opposed by many Republicans, but Democrats have paired it with language barring the use of mandatory arbitration clauses to blunt a person's ability to avail herself of the civil justice system.

EDPB's Review of Privacy Shield

The European Data Protection Board (EDPB or Board), an entity consisting of the European Union's (EU) data protection authorities, has released its annual assessment of the EU-U.S. Privacy Shield and again finds both the agreement itself and implementation wanting. There was some overlap between the concerns of the EDPB and the the European Commission (EC) as detailed in its recently released third assessment of the Privacy Shield, but the EDPB discusses areas that were either omitted from or downplayed in the EC's report. The EDPB's authority is persuasive with respect to Privacy Shield and carries weight with the EC; however, its concerns as detailed in previous annual reports have pushed the EC to demand changes, including but not limited to, pushing the Trump Administration to nominate Board Members to the Privacy and Civil Liberties Oversight Board (PCLOB) and the appointment of a new Ombudsperson to handle complaints about how the U.S. Intelligence Community is handling the personal data of EU citizens. Conceivably, this EDPB assessment could create more pressure for the Department of Commerce (Commerce) and Federal Trade Commission (FTC) to engage in more stringent oversight of those entities attesting to adhering to Privacy Shield in the transfer and processing of the personal data of EU citizens, including FTC actions alleging violations of Section 5 of the FTC Act if entities claim to be certified or in compliance but are found not to be (as the agency did in four recent cases.)

The EDPB took issue with how the Commerce is conducting spot reviews of a business's adherence to Privacy Shield and how the FTC is enforcing the regime. In the view of the EDPB, these checks are mostly formal and do not delve into the substance of whether the business is actually complying with the requirements of Privacy Shield to protect the personal data of EU citizens. In particular, the EDPB criticized the lack of oversight of so-called onward transfers of the EU citizens' data from the EU through the U.S. and into other countries that may not offer the protections required in the EU. The EDPB called for closer scrutiny of this practice by Commerce and for an examination of the contracts U.S. companies enter into with entities in third countries to ensure the requirements of Privacy Shield are being met. The EDPB renewed its concerns about the EU and U.S.'s different readings on how human resources (HR) data are to be treated, namely that EU employees would not be able to avail themselves of the same protections once their data has been transferred to the U.S. The EDPB also expressed its concern about how Commerce handles lapsed certifications of compliance with Privacy Shield by noting that such entities are still listed as being certified. The EDPB pushed for a reformed recertification regime.

The EDPB also expressed its "opinion that it is important that the [EC] continues monitoring cases

related to automated decision making and profiling and to contemplate the possibility to foresee specific rules concerning automated decision making to provide sufficient safeguards, including the right to know the logic involved and to challenge the decision obtaining human intervention when the decision significantly affects him or her." Finally, the EDPB noted "the remaining issues with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016 in particular regarding the absence or the limitation to the rights of the data subjects (i.e. right to object, right to access, right to be informed for HR processing), the absence of key definitions, the application of the principles when it comes to "processors", the lack of guarantees on transfers for regulatory purpose in the field of medical context, the lack of specific rules on automated decision making and the overly broad exemption for publicly available information." The EDPB stated "[t]hose remain valid."

The EDPB also took issue with U.S. law enforcement and national security treatment of EU citizens' personal data. The Board asserted that nothing had changed in the legal landscape in the U.S. since last year's review but recounted its concerns, chiefly that under Title VII of the Foreign Intelligence Surveillance Act (FISA) and Executive Order (EO) 12333 indiscriminate data collection from and analysis of EU citizens could occur with minimal oversight and little to no redress contrary to EU law. However, the EDPB lauded "the now fully functional Privacy and Civil Liberties Oversight Board (PCLOB)" even though many of its crucial reviews of U.S. surveillance practices were classified and therefore off-limits for the Board to review, notably its forthcoming review of EO 12333 which provides an alternative basis for the Intelligence Community to conduct surveillance. Nonetheless, overall, the EDPB calls for more safeguards for U.S. surveillance that would make these activities more targeted. The EDPB also decried how the standing requirements in federal courts have effectively blunted the available redress for EU citizens under the Privacy Act of 1974. The Board also enumerated its concerns about the Ombudsperson "provides the only way for EU individuals to ask for a verification that the relevant authorities have complied with the requirements of this instrument by asking the Ombudsperson to refer the matter to the competent authorities, which include the Inspector General, to check the internal policies of these authorities." The EDPB was concerned about the impartiality and independence of the current Ombudsperson, Under Secretary of State for Economic Growth, Energy, and the Environment Kenneth Krach and asserted "still doubts that the powers of the Ombudsperson to remedy non-compliance vis-a-vis the intelligence authorities are sufficient, as his "power" seems to be limited to decide not to confirm compliance towards the petitioner."

The EDPB detailed its "significant concerns that need to be addressed by both the Commission and the U.S. authorities:"

- As regards the commercial aspects, the absence of substantial checks remains a concern of the EDPB. Other areas that require further attention are the application of the Privacy Shield requirements regarding onward transfers, HR data and the application of the principles when it comes to processors, as well as the recertification process. More generally, the members of the Review Team would benefit from a broader access to non-public information, concerning commercial aspects and ongoing investigations. In addition, the EDPB recalls the remaining issues with respect to certain elements of the commercial part of the Privacy Shield adequacy decision as already raised in the WP 29's Opinion 01/2016.
- As regards the collection of data by public authorities, the EDPB can only encourage the PCLOB to issue and publish further reports. It regrets that on Section 702 FISA no general report is contemplated, to provide an assessment of the changes brought since the last reauthorization in 2018. The EDPB would be very interested on an additional report on

PPD-28 to follow up on the first report including an assessment of how the safeguards of PPD-28 are applied Finally, the EDPB underlines the importance of reports on Executive Order 12333, and regrets that those reports will most likely remain classified. In this regard, the EDPB stresses that the members of the review team only have access to the same documents as the general public. The EDPB recalls that the security cleared experts of the EDPB remain ready to review additional documents and discuss additional classified elements, in order to have more meaningful reviews, following the example of PNRs or TFTP reviews.

- On the Ombudsperson mechanism, despite some new elements provided during this year's review, especially on the procedural aspects in relation to the first case submitted to the Ombudsperson but declared inadmissible, as well as on hypothetical cases, the EDPB is still not in a position to conclude that the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Thus, it still cannot state that the Ombudsperson can be considered an "effective remedy before a tribunal" in the meaning of Art. 47 of the EU Charter of Fundamental Rights.
- Finally, the EDPB recalls that the same concerns will be addressed by the Court of Justice of the European Union in cases that are still pending before it."

House Homeland Security Committee on Election Security

Last week, House Homeland Security Committee's Cybersecurity, Infrastructure Protection, and Innovation Subcommittee held its most recent hearing on the security of U.S. election systems. While there was bipartisan agreement on the need to better secure election systems and numerous suggestions on how to do so, implicit in these talks was the reality that better funding and direction from the federal government are needed, which is a point where agreement begins to diverge. Moreover, the frame through which Republican and Democratic Members viewed interference and disinformation throughout the 2016 election demonstrates the differing views on what happened, its effect, and most crucially necessary remedies. Finally disinformation and misinformation spread on social media platforms was a key component of elections that was discussed with questions posed on how to counter these core tactics of nations like Russia, Iran, and China.

Subcommittee Chair Cedric Richmond (D-LA) stated that the hearing would be "a broad look at election security issues, including efforts from the private sector to protect election infrastructure and political campaigns against malicious actors." He declared that "[i]t is an undisputable fact that, in 2016, the Russian government carried out a concerted, sophisticated operation to meddle in our presidential election." Richmond stated that "[t]he Kremlin leveraged sophisticated cyber capabilities to target our election infrastructure and amplify divisive – and at times false – rhetoric in an unprecedented way to sow discord, undermine the public's faith in democratic institutions, and ultimately damage the global leadership of the United States." He said that "[t]he Russian government's covert malicious foreign interference campaign attacked every aspect of our elections…[and] involved engaging in conversations with personnel from a U.S. presidential campaign, hacking a national political Committee, conducting a phishing attack against a campaign chairman, targeting voter registration databases and other election infrastructure, and mobilizing bots and fake online personas to carry out influence operations."

Richmond stated that "[t]oday, two other nation-state actors, China and Iran, are following suit--weaponizing new technologies to disrupt our democracy, distort the daily news, and compromise our election security." He asserted that "[a]s we move into the heart of the 2020 election cycle, we must set aside party politics and work together to improve election security and preserve the

integrity of our democracy." Richmond said that "[t]o that end, I urge the White House to accept the Intelligence Community's unanimous conclusions about 2016 meddling, refrain from engaging in conspiracy theories ahead of the 2020 elections, and show some needed leadership on election security." He stated that "[f]ailing to do so will further erode public confidence in our election process and advance Vladimir Putin's goal of undermining the US-led liberal democratic order."

Richmond stated that "[f]or its part, Senate leadership must pass House-passed measures that would make election infrastructure more secure, and it should match the House's commitment to funding election security grants." He stated that "[s]ecurity vulnerabilities in outdated, unsupported election infrastructure could jeopardize the accuracy of voter registration databases or even the tally of votes cast…[and] [t]hat is simply unacceptable." Richmond argued that "[v]oters deserve to know that they will be able to vote when they show up, and that their vote will be counted accurately…[and] [t]o guard against covert malicious foreign influence campaigns, owners and operators of online platforms must understand and be candid with the public about how our adversaries use their platforms." He contended that "we need to educate the public so that they are informed and have the opportunity to distinguish between facts and disinformation…[a]nd our party organizations and campaigns must take cybersecurity seriously, monitor for disinformation, and refuse to take advantage of malicious disinformation circulated about their opponents."

Richmond stated that "[p]arty and campaign organizations have tremendous power to counter efforts by foreign adversaries simply by rejecting opportunities to take the cheap shots based on fake news…[and] [t]ogether, those truly interested in defending our elections from foreign adversaries can make real progress." He added that "[f]or example, despite a lack of leadership from the White House, the Department of Homeland Security is building relationships and providing a full suite of election security services to State and local election officials." Richmond asserted that "[i]n addition, Office of the Director of National Intelligence, Federal Bureau of Investigation, National Security Agency, and U.S. Cyber Command have teams to coordinate and integrate election security threat information. " He declared that "[t]he private sector is also stepping up…[c]ybersecurity researchers at non-profit and for-profit organizations are providing cybersecurity services to campaigns and election officials….I commend these efforts."

Subcommittee Ranking Member John Katko (R-NY) claimed that "[s]ecuring our elections remains one of the most pressing issues our country faces…[s]ecure voting systems and the accurate reporting of votes is foundational to our democracy…[and] Americans should have full confidence in every aspect of our election process." He stated that "[u]nfortunately, our election systems have also become the principal target of several adversaries." Katko said that "[d]isinformation campaigns engineered by Russia have sewn political discord within our election process." He added that "[s]ocial media has become a haven for false information regarding election day procedures and misinformation of candidates…[and] [d]isinformation campaigns serve to confuse voters and undermine their confidence in the electoral process."

Katko stated that "[w]hile foreign influence has had a measured effect on our discourse, election results have fortunately remained untouched…[and] [t]he success of the 2018 midterms demonstrated the progress that the federal government and our state and local partners have made." Katko stated that "I want to applaud election security efforts led by the Cybersecurity and Infrastructure Security Agency (CISA) and their partnerships with state and local governments that have resulted in a marked improvement of information sharing and cohesion." He asserted that "growing participation within the Election Infrastructure Information Sharing and Analysis Center

(ISAC) by local election officials has provided thousands of election offices with the cyber resources they need to maintain the reliability of their election infrastructure."

Katko said that "[p]aper trails for voting systems are now in use in all but a few states, providing voters with an incorruptible record of their vote…[and] [t]he continued development of auditing techniques confirms voting results where voter tallies may be called into question." Katko said that "[t]hese software independent techniques have become invaluable to protecting our election systems from cyber-attacks…[and] [s]oftware independence of our election infrastructure is essential for the integrity of our election systems." Katko stated that "[t]his progress does not mean our election systems are secure…[and] [o]ne can imagine the effect of a similar targeted ransomware campaign aimed at voter registration database systems before an election." He added that "[s]uch an attack would hijack our election process and undermine all voter confidence in election results."

Katko stated that "we must continue to develop our relationships with state and local election partners to ensure federal cybersecurity resources are being utilized…[and] [w]hile participation in the Election Infrastructure ISAC has improved since the 2016 elections, thousands of local election offices remain independent. Local election offices are not equipped to handle the cyber threats to their election infrastructure alone." He contended that "[i]t is imperative the federal government makes available its cybersecurity resources to every local election office." Katko said that "[e]lection security has a history of bipartisan cooperation and support…[and] [e]nsuring that our election process is uncompromised must remain a top priority for both sides of the aisle." He stated that "I am confident that we can take the necessary reasonable steps to continually improve our election systems."

Committee Chair Bennie Thompson (D-MS) said that "[s]ince 2016, officials throughout the Intelligence Community have described in disturbing detail the many ways the Russian government sought to meddle in our elections." He asserted that "[f]or the three years that followed, heads of the Department of Homeland Security, the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Security Agency, among others, have warned that the Russian government will continue its efforts to sow discord and undermine confidence in our democracy." Thompson stated that "[m]ore disturbing yet, Russia is not alone." According to the 2019 Worldwide Threat Assessment, other adversaries, including China and Iran, will pursue opportunities to interfere in our elections." He said that "[t]he Intelligence Community assesses that adversaries could exploit cyber means to target election infrastructure or engage in targeted influence campaigns to manipulate public opinion."

Thompson stated that "[w]e also know that our adversaries will target political campaigns because they have done so in the past…[and] [o]ur adversaries have hardly kept their desire to undermine the integrity of our elections a secret." He said that "[a]s Members of Congress, we have a duty to act…[and] [t]he question everyone on this dais must ask themselves is: "Have we done enough to secure the 2020 elections from our adversaries?" Thompson stated that "[d]espite multiple efforts led by the House of Representatives, Congress has yet to send a single piece of comprehensive election security legislation to the President's desk." He said that "[i]nstead, good pieces of legislation to provide additional resources to State and local election officials and limit foreign interference have stalled in the Senate." Thompson stated that "[m]oreover, despite multiple requests, the White House has failed to identify an official to coordinate the election security activities at various Federal agencies." He asserted that "[i]n the meantime, we have just a handful of legislative days left this year, and only a limited amount of time for legislative action next year."

Thompson stated that "I will be interested to know how academics and the private sector can work with State and local elections officials and campaigns to improve election security in the absence of Congressional action." He said that "[t]he election security problems we face are shared, and we have a shared responsibility to solve them…[and] [s]tate and local election authorities –with help from the Federal government –must invest in IT departments, train their employees, and upgrade and certify their election equipment." Thompson asserted that "[t]he private sector, including voting system vendors, must take responsibility to secure their equipment, make it user-friendly, and demonstrate a willingness to admit weaknesses in their systems when examined by third-party cybersecurity professionals." He said that "[p]olitical campaigns must step up, too…[and] [t]hey must implement robust cybersecurity policies to deprive our adversaries of information that can be twisted into a divisive narrative and serve as an extra check on disinformation." Thompson stated that "the American public must also be vigilant, and scrutinize the information presented to them carefully."

Former Under Secretary of Homeland Security for Intelligence and Analysis and US CyberDome Executive Director pro tempore General Frank Taylor identified the following as possible responses to the threats posed by nation states against U.S. elections and campaigns:

- *Capitalize on the non-profit model*. Non-profit organizations are uniquely positioned and scoped to support campaigns. Specifically, non-profits avoid misgivings campaigns may have about utilizing federal government and for-profit resources directly. When non-profits engage campaigns, it reduces risks they may face, and we all face, if those campaigns are isolated. Non-profits are not a part of the executive brand of government, therefore they are not affiliated with a competing candidate. Non-profits less prone to the financialc onflicts of interest faced by a for-profit. At the same time, non-profits can still play an integral role in brokering the resources of the federal government and for-profit organizations. For instance, non-profits may offer an indirect way to disseminate cyber threat information (and do so in formats that can be immediately utilized by campaigns). For all of these reasons, I believe non-profit organizations are well-suitedt o support political committees and campaigns with on-going and proactive measures.
- *Specify minimum standards for campaign cybersecurity*. Campaigns may have greater incentive to spend effort and funds on cyber protections if they know their competitors are obligated to the same expenditures. Here is a similar circumstance from recent history. In the past, US CyberDome personnel helped create the DOD-Defense Collaborative Information Sharing Environment(DCISE). The DCISE stemmed from the Comprehensive National Cybersecurity Initiative to be one of the first successful examples of "need to share" in America.
- *Focus on key technical challenges*. Congress should consider mandating that all U.S. government threat intelligence be disseminated in computer-readable formats, in addition to prose. This simple requirement would go a long way to ensuring that action can be taken swiftly once threat intelligence information is received. I do not espouse a specific format. I would leave that up to the experts. Expressing all threat information in computer-readable formats will be a big step forward. Challenges like de-classification are more complex to solve. Over-classification is something that intelligence organizations should evaluate for themselves. In other words, is it possible that certain aspects of the threat information never needed to be classified to begin with? Accelerating de-classification should also be considered. We are living in an age where machine learning is broadly applied, and artificial intelligence is starting to be well-understood. These technologies hold significant promise to automate large portions of the de-classification process.

Former Under Secretary of State for Public Diplomacy and Public Affairs Richard Stengel stated that "[e]ven though I don't think government has much of a role in countering disinformation through creating content or taking it down, I do think there is a clear government role in raising awareness and creating resilience to disinformation." He asserted that "[c]ombatting disinformation is a cross-cutting issue that has implications for a wide range of different agencies and committees. " Stengel stated that "[f]irst, I think government has a role in regulating the platforms that host disinformation…[and] [c]urrently, there is an alignment of economic interests between the disinformationists and the platforms: the social media companies make money when disinformation goes viral." He explained that "[r]ight now, the law doesn't treat the platform companies as publishers and they have complete immunity from liability for the content on their platforms…[and] [n]ot only are these companies publishers, they are the biggest publishers in the history of the world." Stengel stated that "[t]o be sure, these companies cannot have the same liability that I used to have as editor of TIME…[b]ut they need to have some liability for content that is on their platform that is demonstrably false, that is created by robots, that attacks others on the basis of race, religion, ethnicity, gender or sexual orientation, that is created by foreign actors to deceive American voters." He contended that "[t]hey need to be legally accountable for making a good faith effort to remove such content from their platforms."

Stengel stated that "[a]s the 2020 election approaches, there are a host of new problems: deep fakes; data manipulation, where bad actors don't steal data but manipulate it; the professionalization of interference, as private companies hire out their services to create disinformation; the rise of domestic disinformation and the recruiting of Americans as witting or unwitting agents of disinformation." He stated that "[c]ombatting these new efforts requires the detection and removal of foreign influence in our election, greater ad transparency, more accountability for the platform companies, and greater data protection." Stengel said that "I would endorse the Senate Intelligence Committee's recommendations for fighting disinformation, and in particular the timely sharing of information between the private and public sector of real-time threats…[and] I believe the tech companies would welcome that too." He stated that "I'd also recommend the Five D's of combatting disinformation: detection, demotion, deletion, disclosure and digital literacy."

Stengel stated that "[t]he disinformationists know that it's far easier to create confusion rather than clarity, to confuse rather than persuade…[and] [t]hey want people to see empirical facts as an elitist conspiracy." He claimed that "[c]itizens have trouble discerning fact from fiction and we need to teach media and digital literacy in the schools from an early age. In a new poll from this past week, 47% of Americans say they find it difficult to know whether the information they encounter is true." Stengel stated that "[t]he public needs to see that countering disinformation is a civic duty for which we all are responsible." He declared that "[u]ltimately, the problem of disinformation is not so much that people will come to believe what is false…[and] [t]he greatest problem is that they it will cause them to question what is true."

Georgetown University Professor Matt Blaze offered "three specific recommendations:

- Paperless (DRE) voting machines should be phased out from US elections immediately, and urgently replaced with precinct-counted optical scan ballots that leave a direct artifact of voters' choices.
- Statistically rigorous "risk limiting audits" should be routinely conducted after every election, in every jurisdiction, to detect and correct software failures and attacks.

- State and local voting officials should receive access to significant additional resources, infrastructure, and training to help them protect their election management IT systems against increasingly sophisticated adversaries.

Microsoft's Defending Democracy Program's Strategic Projects Director Ginny Badanes stated that

- Beyond culture setting, Congress also can contribute to a multi-stakeholder approach to addressing the threats themselves. We believe that combatting attacks will require a joint effort from private sector actors such as Microsoft, as well as state, local and federal governments, civil society, academia, and campaign organizations themselves.
- Cyber-attacks, especially ransomware attacks, are increasingly targeting state and local authorities, including for example, Atlanta (GA), Baltimore (MD), Cleveland (OH), Greenville (NC), Imperial County (CA), Stuart (FL), Augusta (ME), Lynn (MA), Cartersville (GA). Most recently there was an attack on over twenty government entities in Texas. Overall, we can reasonably expect that the situation will only get worse. Importantly, these and other attacks are increasingly leveraging sophisticated tools that are developed by governments, creating a dangerous ecosystem of cyber-weapons and requiring adoption of international norms for responsible behavior online. Microsoft advances support for the adoption and observance of such norms.
- Microsoft supports the multi-stakeholder approach taken by the Paris Call for Trust and Security in Cyber Space. It reaffirms a number of norms and principles established in other forums, including at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN-GGE), and at the G7 and G20, respectively. Importantly, the Paris Call includes a comparatively new principle to protect electoral processes from foreign interference – "*Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.*"
- However, what truly distinguishes the Paris Call is that it recognizes that a multi-stakeholder approach is essential to achieve success. The Call has so far been endorsed by over 1000 signatories, the largest coalition of signatories ever in support of a cybersecurity document: 74 governments, 357 civil society and public sector organizations, and 607 industry members all agreeing to nine core principles to govern conduct in cyberspace. Microsoft was one of the private sector signatories and we will continue to advocate that all governments agree to observe the nine principles of the Call.
- While we are here today to discuss campaign organizations, we'd be remiss not to address other ways Congress can support securing our elections. In our discussions with voting officials around the country we have learned that consistent and reliable funding over time will best enable election officials to plan ahead, purchase new equipment rather than letting outdated systems remain active, and invest in the kind of cybersecurity training and staffing that we expect of all critical infrastructure owners and operators. Our adversaries are relentless and well resourced. To ensure we can maintain defenses, our state and local voting officials need a durable source of federal financial support so that the most secure technology can be deployed rapidly to ensure our vote is protected. The stewardship of our democracy demands nothing less.

Commerce Issues Draft Regulations On Information and Communications Technologies and Services

The Department of Commerce (Commerce) has released its long-awaited draft regulations as required by a May 2019 executive order that would implement a case-by-case review process for

information and communications technology and services (ICTS) that pose unacceptable risks to U.S. national security or the safety of Americans. While the executive order provided Commerce with the authority to exempt classes of ICTS, it has chosen not to do so at this point. In the same vein, Commerce could have found that a class of technology or services posed undue risks and, per the EO, could have summarily barred the import and sale of these items. And yet, Commerce has not chosen to do that either even though it would have likely pleased many in Congress if Commerce had barred Huawei, ZTE, and other Chinese services and products. Nonetheless, comments are due by December 27, 2019.

In May 2019, the President issued Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," (EO) 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.

Per the direction in the EO, Commerce "proposes to implement regulations that would govern the process and procedures that the Secretary of Commerce (Secretary) will use to identify, assess, and address certain information and communications technology and services transactions that pose an undue risk to critical infrastructure or the digital economy in the United States, or an unacceptable risk to U.S. national security or the safety of United States persons." Specifically, the EO "grants the [Commerce] the authority to prohibit any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (a "transaction") subject to United States' jurisdiction where the Secretary, in consultation with other relevant agency heads, determines that the transaction:

> (i) Involves property in which a foreign country or national has an interest;
> (ii) includes 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
> (iii) poses certain undue risks to critical infrastructure or the digital economy in the United States or certain unacceptable risk to U.S. national security or U.S. persons.

Commerce is proposing "a process by which the Secretary will determine whether a particular transaction should be prohibited." Commerce stated that "[a] transaction that meets the following conditions will be subject to review by the Secretary and may require mitigation, prohibition, or an unwinding of the transaction if determined to be prohibited:

> (1) The transaction is conducted by any person subject to the jurisdiction of the United States or involves property subject to the jurisdiction of the United States;
> (2) the transaction involves any property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of the technology or service); and
> (3) the transaction was initiated, pending, or completed after May 15, 2019, regardless of when any contract applicable to the transaction was entered into, dated or signed, or when any license, permit, or authorization applicable to such transaction was granted. Transactions involving certain ongoing activities, including but not limited to managed

services, software updates, or repairs, would constitute transactions that was completed on or after May 15, 2019 even if a contract was entered into prior to May 15, 2019.

Commerce is therefore proposing "a case-by-case, fact-specific approach to determine those transactions that meet the requirements set forth in the Executive order and are therefore prohibited or must be mitigated...[that] allows for the deliberative application of the authority granted to the Secretary by the President in the EO as the Secretary seeks to calibrate properly the application of this new authority." Commerce contended that "[a] case-by-case application of this authority would allow the Secretary to target and prohibit transactions that meet the EO criteria, without unintentionally prohibiting other transactions involving similar ICTS that may not rise to the level of presenting an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to national security or the safety of U.S. persons." Commerce asserted that "[t]his approach would also ensure that the Department does not inadvertently preclude innovation or access to technology in the United States."

In terms of implementation, Commerce will decide whether the particular circumstances of a potentially prohibited transaction may meet" [the above three-part criteria]. Commerce may initiate this process, or at the behest of another federal agency, including the Federal Acquisition Security Council (FASC). In either case, Commerce will determine whether the identified transaction should be prohibited or mitigated in consultation with other agencies as necessary. Commerce would notify the parties involved in the flagged transaction once a preliminary decision has been made and the bases for the determination. Commerce "would assess, for example, whether a party to a transaction is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, and whether the use of a certain class of ICTS or transactions by particular classes of users present an undue or unacceptable risk." Within 30 days after being notified of a determination, a party may submit its opposition and information arguing against the agency's finding. 30 days after receiving such a submission, Commerce must issue its final decision to either prohibit the transaction; not prohibit the transaction; or "require measures and specific timeframes to mitigate risks identified during an evaluation as a precondition of approving a transaction that may otherwise be prohibited." In any event, this determination must be in writing and an unclassified version would be released, and Commerce would safeguard and not release any classified information involving the transaction or the deliberative process.

Finally, as noted, Commerce opted against excluding or exempting any classes of ICTS at this time: The EO also authorizes the Secretary to exempt certain classes of transactions from the EO's restrictions if the Secretary determines (for example, because of the nature or capabilities of the ICTS involved or the characteristics of the purchaser or ultimate user) that such transactions do not present an undue or unacceptable risk or are outside the scope of the EO. The EO also authorizes the Secretary to prohibit transactions as a class if the Secretary determines that such class of transactions pose an undue or unacceptable risk. The proposed rule does not recognize particular technologies or particular participants in the market for ICTS as categorically included or excluded from the prohibitions established by the EO. If, in the future, the Secretary determines that it is appropriate to designate classes of transactions for categorical inclusion or exclusion, further guidance will be issued at that time.

Bill Introduced Aimed At Chinese and Russian Technology Companies

Senator Josh Hawley (R-MO) has released a bill, the "National Security and Personal Data Protection Act of 2019," (S. 2889) that is a bit of a Franken-bill in that it marries provisions aimed

at Chinese and Russian ICT entities, and by extension the government in Beijing, with some provisions from privacy and data security bills. Technology companies operating in or outside of those countries, including subsidiaries or other entities controlled by the parent company, would not be able to transfer U.S. user data to China or Russia directly or indirectly, must minimize any such data collection and processing, and would be barred from any data processing beyond the original purpose for which it was collected. Other technology companies such as U.S. entities would not be able to transfer user data to China or Russian and would not be able to store user data there either.

The bill lists the countries of concern as China and Russia with the caveat that the Secretary of State may identify more. And, it is the technology companies operating in, from, and on behalf of these countries that the bill aims its restrictions. Covered technology companies are "online data-based service such as a website or internet application...organized under the laws of a country of concern...[or] in which foreign persons that are nationals of, or companies that are organized under the laws of, countries of concern have a plurality or controlling equity interest" or is a subsidiary two the two aforementioned types of companies. Additionally, a covered technology company could be "otherwise subject to the jurisdiction of a country of concern in a manner that allows the country of concern to obtain the user data of citizens and residents of the United States without similar respect for civil liberties and privacy as provided under the Constitution and laws of the United States." This last provision may be designed–or to be fair, it may be inadvertent–to sweep in a number of U.S. companies that don't fall into the other categories.

Covered technology companies would be subject to new responsibilities and duties. These entities may "not collect any more user data than is necessary for the operation of the website, service, or application of the company." Covered technology companies are further barred from utilizing user data for "any purpose that is secondary to the operation of the website, service, or application of the company, including providing targeted advertising, unnecessarily sharing such data with a third party, or unnecessarily facilitating facial recognition technology." These entities may not "transfer any user data or information needed to decipher that data, such as encryption keys, to any country of concern (including indirectly through a third country that is not a country of concern)." Likewise, covered technology companies would not be allowed to "store any user data collected from citizens or residents of the United States or information needed to decipher that data, such as encryption keys, on a server or other data storage device that is located outside of the United States or a country that maintains an agreement with the United States to share data with law enforcement agencies through a process established by law." However, there is a carve out in that the aforementioned restrictions "shall not apply where data is collected, used, retained, stored, or shared by a covered technology company solely for the purpose of assisting a law enforcement or military agency that is not affiliated with a country of concern." However, there is no exception for the prohibition on data storage in a country of concern even for the military or law enforcement.

Moreover, any user of the services of a covered technology company would have the following rights:

- To "view any user data held by the company that relates to the individual; and
- To "permanently delete any user data held by the company that has been collected, directly or indirectly, from the individual."

However, user created content such as TikTok clips, YouTube content, Instagram, etc would be exempted from the prohibitions on transferring data to and data storage in a country of concern.

There are a different set of restrictions for "any company operating in or affecting interstate or

foreign commerce that provides a data-based service such as a website or internet application but is not a covered technology company" (e.g. Facebook, Amazon, and many others.) These companies may "not transfer any user data collected from an individual in the United States or information needed to decipher that data, such as encryption keys, to any country of concern (including indirectly through a third country that is not a country of concern)." These companies also may "not store any user data collected from an individual in the United States or information needed to decipher that data, such as encryption keys, on a server or other data storage device that is located in any country of concern." There would be similar carve outs for law enforcement and military in that the data transfer and storage prohibitions would not apply "solely for the purpose of assisting a law enforcement or military agency that is not affiliated with a country of concern" and for user created content.

The Federal Trade Commission (FTC) would enforce the new regime and would be empowered to levy civil fines as high as $42,530 per violation. Moreover, there would criminal liability for knowingly violating the prohibitions placed on covered technology companies (i.e. Chinese or Russian entities) or other technology companies of up to 5 years in prison and civil fines. Like many privacy and data security bills, state attorneys general could enforce the new statute, and any person harmed by a covered technology company by way of violating this act would have the right to sue for civil damages of $1,000 per violation with a cap of $25,000 along with other relief.

Finally, foreign companies looking to buy, take over, or invest in U.S. companies collecting, processing, and disclosing user data would be made subject to CFIUS review. Specifically, these transactions would include for any company "that collects, sells, buys, or processes user data...and whose business consists substantially more of transferring data than manufacturing, delivering, repairing, or servicing physical goods or providing physical services" and any that operate a social media platform or website.

FCC Approves Final Rule Barring Use of Funds To Buy Chinese Telecom Equipment

On November 22, Federal Communications Commission (FCC) agreed to a Report and Order that "would prohibit companies from using money from the FCC's $8.5 billion Universal Service Fund (USF) to purchase equipment or services from any company that poses a national security threat" and "would initially designate two Chinese companies—Huawei and ZTE Corporation—as companies that pose a national security risk and would establish a process for designating additional covered companies in the future" according to a fact sheet. This rule is prospective, so it affects future uses of USF funds to buy or maintain telecommunications equipment. Moreover, the final Report and Order follows a 2018 notice of proposed rulemaking (NPRM) titled "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs" the agency undertook after Congress directed federal agencies to stop buying Huawei and ZTE products and services pending the promulgation of regulations.

Regarding the final rule, the FCC explained

- Based on our review of the extensive record in this proceeding, we adopt a rule that no universal service support may be used to purchase or obtain any equipment or services produced or provided by a covered company posing a national security threat to the integrity of communications networks or the communications supply chain. Accordingly, USF recipients may not use USF funds to maintain, improve, modify, operate, manage, or otherwise support such equipment or services in any way, including upgrades to existing equipment and services.

- In addition to adopting this rule, we initially designate Huawei Technologies Company and ZTE Corporation as covered companies for the purposes of this prohibition. Both companies' ties to the Chinese government and military apparatus—together with Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their systems—pose a threat to the security of communications networks and the communications supply chain and necessitate taking this step. Our actions today are informed by the evidence cited herein, including the actions of other agencies and branches of the government and similar assessments from other countries.

Moreover, included with the draft Report and Order is a Further Notice of Proposed Rulemaking (NPRM) and Information Collection Order that "would propose to remove and replace equipment produced by covered companies from USF-funded communications networks." This NPRM would entail

- An assessment to find out how much Huawei and ZTE equipment is in these networks and the costs to remove and replace it; and
- Financial assistance to carriers to help them transition to more trusted suppliers.

The FCC stated

> In addition to conditioning future USF support, we propose to require eligible telecommunications carriers (ETC) receiving USF support to remove and replace covered equipment and services from their network operations. To mitigate the impact on affected entities, and in particular small, rural entities, we propose to establish a reimbursement program to offset reasonable transition costs. We propose to make the requirement to remove covered equipment and services by ETCs contingent on the availability of a funded reimbursement program. We appreciate that many small and rural carriers affected by today's Report and Order are already committed to securing the integrity of their networks, and we expect these proposals would facilitate the transition of their equipment and services to safer and more secure alternatives and seek comment on these proposals.

In his statement, FCC Chair Ajit Pai stated

- we adopt a ban on using funds from the FCC's USF to purchase equipment or services from companies posing a national security threat to the integrity of communications networks or the communications supply chain.
- We also initially designate two Chinese companies—Huawei and ZTE—as "covered" companies for purposes of this rule, and we set up a process for designating additional such companies in the future.
- We take these actions based on evidence in the record as well as longstanding concerns from the executive and legislative branches about the national security threats posed by certain foreign communications equipment manufacturers, most particularly Huawei and ZTE. Both companies have close ties to China's Communist government and military apparatus. Both companies are subject to Chinese laws broadly obligating them to cooperate with any request from the country's intelligence services and to keep those requests secret. Both companies have engaged in conduct like intellectual property theft, bribery, and corruption.
- Moreover, we know that hidden "backdoors" to our networks in routers, switches, and other network equipment can allow a hostile adversary to inject viruses and other malware, steal Americans' private data, spy on U.S. companies, and more. Indeed, just last month, the European Union found 5G security risks where a "hostile state actor exercises pressure over

> a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities."

FCC Commissioner Jessica Rosenworcel said in her statement:

> I support this effort. I also appreciate that my colleagues were willing to consider changes I offered to the decision and rulemaking we adopt today. In critical part, those include exploring our authority over carriers under the Communications Assistance for Law Enforcement Act to expand our prohibition beyond just the universal service program; providing additional guidance to companies so that our rules do not needlessly disrupt day-to-day service and operations in rural America; implementing the lessons learned from the 600 MHz incentive auction in order to maximize funds available for replacing insecure equipment; and seeking to accelerate the FCC's review of a reimbursement program.

Rosenworcel stated "[s]o while I approve today's decision and rulemaking, I think the FCC has more work to do when it comes to network security." She asserted that "[b]ecause our present efforts to remove and replace insecure equipment are not bold enough…[and] [w]e need a coordinated, national plan for managing the future of 5G security—and the evidence all around us makes crystal clear we don't have one."

In advance of the November 22 open meeting, FCC Commissioner Geoffrey Starks released a report titled "Security Vulnerabilities Within Our Communications Networks" that summarized a July 27 workshop "to consider security threats that stem from the presence of certain Chinese communications equipment in U.S. networks and from the related services these companies provide." Starks stated

> A major takeaway from the workshop is that our networks must only contain equipment from trusted sources. When evaluating the security of a piece of communications networking equipment we should not ask "do I trust this piece of equipment" but instead, "do I trust the manufacturer?" Because networking equipment today relies so heavily on software from its manufacturer, no equipment from an untrustworthy manufacturer should be used. Even if the equipment appears secure at first, if a manufacturer must comply with the Chinese national security law by providing "front door" access to the Chinese government via upgrades and patches, then no amount of mitigation will fully address the problem.

OMB Sets FISMA and Privacy Policy Metrics

The Office of Management and Budget (OMB) has released its "Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements" that is binding on civilian agencies and defense agencies only with respect to non-national security systems. Through this memorandum, OMB is setting "reporting guidance and deadlines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA)." Of course, this is one of the major levers OMB uses to drive information security and privacy policy throughout the civilian federal government, one that directly informs the FISMA metrics Congress closely reviews annually to get a sense of how well or poorly agencies are faring. OMB claimed that the memorandum "also consolidates several government-wide reporting requirements to eliminate duplicative or burdensome processes in accordance with the requirements in Office of Management and Budget (OMB) Memorandum M-17-26, Reducing Burden for Federal Agencies by Rescinding and

Modifying OMB Memorandum." Additionally, OMB rescinds last year's FISMA and privacy requirements, too.

OMB stated that it and the Department of Homeland Security (DHS) "will use CIO and IG metrics to compile the Annual FISMA Report to Congress and may use this reporting to compile agency-specific or government-wide risk management assessments as part of an ongoing effort in support of Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

The FY 2019 CIO Metrics "focus on assessing agencies' progress toward achieving outcomes that strengthen Federal cybersecurity...[and] [i]n particular, the FISMA metrics assess agency progress by:

1. Ensuring that agencies implement the Administration's priorities and best practices;
2. Providing the OMB with the performance data to monitor agencies' progress toward implementing the Administration's priorities."

However, OMB explained
Reflecting the Administration's shift from compliance to risk management, as well as the guidance and requirements outlined in OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program, and Binding Operational Directive 18-02, Securing High Value Assets, CIO Metrics are not limited to assessments and capabilities within National Institute of Standards and Technology (NIST) security baselines, and agency responses should reflect actual implementation levels. Although FISMA requires an annual IG assessment, OMB strongly encourages CIOs and IGs to discuss the status of information security programs throughout the year.

Similarly, the FY 2019 Inspector General's FISMA Metrics "provide reporting requirements across key areas to be addressed in the independent evaluations of agencies' information security programs."

In the main, the section on Incident Reporting Requirements tracks last year's memorandum, including the same definition of "major incident" that triggers a reporting responsibility for a covered agency. The same is true of the section "Strengthening Continuous Diagnostics and Mitigation Capabilities."

Further Reading

- "Big Tech's Big Defector" – *The New Yorker*. Roger McNamee was one of the pioneer investors in Silicon Valley, including companies like Facebook, and now condemns many of the data privacy practices the largest technology engage in. This article surveys a number of possible remedies, including banning transfers of data to third parties, imposing a fiduciary duty of companies that collect and process data, and levy a tax on injurious collection and divisive content on platforms.
- "UN Secretary-General: US-China Tech Divide Could Cause More Havoc Than the Cold War" – *WIRED*. Secretary-General António Guterres predicts that a major war could be started with one country utilizing a cyberattack on another country. In this wide-ranging interview, Guterres opines on autonomous weapons, geostrategic social and technological divides. Also, on how technology can help and hurt humans and the flourishing of democracy.
- "The California DMV Is Making $50M a Year Selling Drivers' Personal Information" – *VICE*. Even with the pending effective date of the "California Consumer Privacy Act," there is a

significant loophole through which sensitive data about Californians is being sold to data brokers and others: the DMV. In a public records request, VICE found out the DMV earned $50 million last year selling such data, and California is not the only state doing this.

- "Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone." – *The New York Times*. An eye-opening investigation on the huge gap between the technological and legal resources available to prosecutors and largely out of reach for public defenders. Even though smartphones and the trove of data they hold could better help courts get to the truth of many criminal matters, public defenders are either not able to afford technology prosecutors typically use to extract data from phones but they also cannot issue warrants to tech companies which frequently rebuff the subpoenas they issue. As a side note, one company, Grayshift, offers technology to prosecutors to access the data on encrypted iPhones, suggesting there are means for law enforcement to break encrypted communications.
- "Exclusive: China's ByteDance moves to ringfence its TikTok app amid U.S. probe – sources" – *Reuters*. In the face of a Committee on Foreign Investment in the United States (CFIUS) review, TikTok's parent, ByteDance, is reportedly putting in place systems to ensure separation between the data collected by TikTok and the data collected by the parent company.
- "U.S. Tech Companies Prop Up China's Vast Surveillance Network" – *The Wall Street Journal*. Through minority partnerships or other arrangements, the technology of a number of American firms are being used by Chinese firms to assist in surveillance and oppression in China. The U.S. firms typically claim not to know the end uses but profess their opposition to the types of tactics used in China.