Technology Policy Update
14 November 2019
By Michael Kans, Esq.

A Privacy Bill A Week: Online Privacy Act of 2019

Last week, we dived into the last White House on privacy, the discussion draft of the "Consumer Privacy Bill of Rights Act of 2015" released by the Obama Administration. This bill was released in conjunction with a report on privacy issues and then proceeded to go nowhere as there was scant appetite on Capitol Hill to legislate on privacy. Let us flash forward to the present where privacy has moved to the fore, and the first of the long-anticipated privacy bills has been released.

Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA) unveiled the "Online Privacy Act of 2019" (H.R. 4978), which they started working on earlier this year when it seemed clear that the House Energy and Commerce Committee's effort to craft a bill had stalled as Consumer Protection and Commerce Subcommittee Chair Jan Schakowsky's (D-CA) timeline for when a bill might be unveiled continued to repeatedly slip. It must be said that this bill is going to be a non-starter with Republicans in the Senate and White House not least of which because it gives consumers a private right of action, creates a new federal agency to police data security, and does not preempt state statutes. Moreover, given Eshoo's close political relationship with Speaker Nancy Pelosi (D-CA), this bill may be viewed in two contexts: 1) Pelosi may approve of the substance of the bill; and 2) in not trying to dissuade Eshoo and Lofgren, the Speaker may have intended to prod House Energy and Commerce to produce a bill. Finally, it bears note that Eshoo challenged current House Energy and Commerce Chair Frank Pallone Jr when former Representative Henry Waxman (D-CA) stepped down as the top Democrat, and relations between the two reportedly remain affected by the bruising contest. In any event, it is a comprehensive bill that takes a number of new approaches on some of the aspects of privacy and data security, and Eshoo and Lofgren also released a one-page summary and a section-by-section summary.

Big picture, the bill would create a new agency to oversee a new privacy and security regime, the United States Digital Privacy Agency (DPA), meaning, that unlike virtually every other privacy bill, the Federal Trade Commission (FTC) would not be the primary enforcer. However, there may still be a role for the FTC to play as discussed below. The bill unites privacy with data security, which has been a policy preference of a number of high-profile Democrats including Schakowsky and Senate Commerce, Science, and Transportation Committee Ranking Member Maria Cantwell (D-WA). Republicans have been lukewarm on this notion, however. Moreover, express, affirmative consent would generally be needed before most businesses could collect, process, maintain, or disclose a person's personal information subject to a number of exceptions. Businesses would need to state clearly and concisely their privacy and security policies, be responsive to people exercising their rights visa vis their data, and closely supervise the service providers and third-parties with whom personal information is disclosed.

As always, it is crucial to digest the key definitions for this will inform the scope of the Act. Those entities covered by the "Online Privacy Act of 2019" is a broad group, spanning most businesses in the U.S: "a person who…intentionally collects, processes, or…maintains personal information; and…sends or receives such personal information over the internet or a similar communications network." There are two crucial exemptions: 1) people not engaged in commercial activities and

those engaging in commercial activities that is considered "de minimis;" and 2) small businesses, which are defined as entities not selling personal information, earning less than 50% of revenue from processing personal information for targeted or behavioral advertising, not having held the personal data of 250,000 or more people in the last six months, having 200 or fewer employees, and earning $25 million or less in gross revenue in the preceding year. If a small business's status changes, and it crosses the threshold into being a covered entity, then there is a nine-month grace period before it must begin complying the Act.

Besides covered entities, two other classes of entities figure prominently in the bill: "service providers" and "third-parties." A "service provider" is a "covered entity" that generally "processes, discloses, or maintains personal information, where such person does not process, disclose, or maintain the personal information other than in accordance with the directions and on behalf of another covered entity." A third-party is "a person…to whom such covered entity disclosed personal information; and…is not…such covered entity…a subsidiary or corporate affiliate of such covered entity…or…a service provider of such covered entity." Consequently, almost all disclosures of personal information made by a covered entity would likely be to either a service provider or a third party, the latter of which can be a covered entity itself.

The bill defines "data breach" in fairly standard terms as "unauthorized access to or acquisition of personal information or contents of communications maintained by such covered entity." This term has evolved over the last decade to include mere access as opposed to exfiltration or acquisition. The Act coins a new term to cover some possible privacy violations: "data sharing abuse." This means "processing, by a third party, of personal information or contents of communications disclosed by a covered entity to the third party, for any purpose other than—

- a purpose specified by the covered entity to the third party at the time of disclosure; or
- a purpose to which the individual to whom the information relates has consented."

Personal information is simply and very comprehensively defined as "any information maintained by a covered entity that is linked or reasonably linkable to a specific individual or a specific device, including de-identified personal information and the means to behavioral personalization created for or linked to a specific individual." Moreover, "personal information" does not include "publicly available information related to an individual" or "information derived or inferred from personal information, if the derived or inferred information is not linked or reasonably linkable to a specific individual." Under this definition, is there an inadvertent loophole created whereby information not maintained by a covered entity is not personal information for purposes of this Act, and therefore, such information would be beyond many of the requirements of the Act?

The bill uses the definition of "contents" of a communication from the "Electronic Communications Privacy Act" (ECPA) (P.L. 99-508) that is used for wiretapping and electronic surveillance, among other purposes, which shows the intent to allow the legal structure for government surveillance to coexist frictionless alongside the new privacy regime. However, most metadata, which includes the call detail records currently being debated regarding reauthorization of National Security Agency authority, would be covered at a lesser level by this Act, meaning private sector entities could collect, process, maintain, and disclose metadata.

De-identified information are generally those data "that cannot reasonably identify, relate to, describe, reference, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or device." However, this definition stipulates further conditions that must be met: "provided that a business that uses de-identified information—

- has de-identified the personal information using best practices for the types of data the information contains;
- has implemented technical safeguards that prohibit re-identification of the individual with whom the information was linked;
- has implemented business processes that specifically prohibit re-identification of the information;
- has implemented business processes to prevent inadvertent release of de-identified information; and
- makes no attempt to re-identify the information."

This language is going in the right direction, for de-identification of personal information will likely need to be permanent or as close to permanent as possible to forestall the temptation some entities will invariably face to re-identify old personal information and derive value from it.

The "Online Privacy Act of 2019" spells out what constitutes a "privacy harm" and a "significant privacy harm," two key definitions in helping covered entities gauge the sensitivity of certain information and their legal obligations in handling such information. "Privacy harm" is "adverse consequences or potential adverse consequences to an individual or society arising from the collection, processing, maintenance, or disclosure of personal information." Such harms are identified in the definition and worth quoting in full:

- direct or indirect financial loss or economic harm;
- physical harm;
- psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;
- adverse outcomes or decisions with respect to the eligibility of an individual for rights, benefits, or privileges in employment (including hiring, firing, promotion, demotion, and compensation), credit and insurance (including denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;
- stigmatization or reputational harm;
- price discrimination; other adverse consequences that affect the private life of an individual, including private family matters and actions and communications within the home of such individual or a similar physical, online, or digital location where such individual has a reasonable expectation that personal information will not be collected, processed, or retained;
- chilling of free expression or action of an individual, group of individuals, or society generally, due to perceived or actual pervasive and excessive collection, processing, disclosure, or maintenance of personal information by a covered entity;
- impairing the autonomy of an individual, group of individuals, or society generally; and
- other adverse consequences or potential adverse consequences, consistent with the provisions of this Act, as determined by the Director

This list of privacy harms is as expansive, and perhaps even more so, than almost any other bill analyzed. Additionally, this list is not comprehensive, and the DPA may add other harms.
A related, crucial definition is that of "significant privacy harm" which is "adverse consequences to an individual arising from the collection, processing, maintenance, or disclosure of personal information, limited" to three specific privacy harms:

- direct or indirect financial loss or economic harm;

- physical harm; and
- adverse outcomes or decisions with respect to the eligibility of an individual for rights, benefits, or privileges in employment (including hiring, firing, promotion, demotion, and compensation), credit and insurance (including denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services."

A term related to these two is "protected class," which is "the actual or perceived race, color, ethnicity, national origin, religion, sex (including sexual orientation and gender identity), familial status, or disability of an individual or group of individuals."

The Act intends to create a safe harbor for many of the notice and consent requirements that will encourage greater use of encryption or similar methods that would make personal information and the contents of communications very hard to access. To this end, the bill defines a term "privacy preserving computing" as "the collecting, processing, disclosing, or maintaining of personal information that has been encrypted or otherwise rendered unintelligible using a means that cannot be reversed by a covered entity, or a covered entity's service provider," subject to further requirements. Additionally, the DPA "may determine that a methodology of privacy preserving computing is insufficient for the purposes of this definition," so covered entities and service providers would not be free to deem any security measure "privacy preserving computing."

The Act also makes clear that a covered entity's sharing of personal information with a third party for any sort of remuneration will be a sale or selling, and hence the definition is "the disclosure of personal information for monetary consideration by a covered entity to a third party for the purposes of processing, maintaining or disclosing such personal information at the third party's discretion."

Now, let's turn to the substance of the Act. The bill makes clear that no one may waive its requirements, and any contracts or instruments to do so are null and void. Additionally, no one may agree to any pre-dispute arbitration under this bill, meaning that no person will be forced to accept mandatory arbitration as is often the case when one agrees to the terms of service for an application or to use a device.

The "Online Privacy Act of 2019" would take effect one year after enactment, but there is curious language making clear the effective date does not "affect[] the authority to take an action expressly required by a provision of this Act to be taken before the effective date."

The Act carves out journalism from the privacy and security requirements of the bill to the extent an organization like *The New York Times* is engaged in bona fide journalism as opposed to other commercial activities such as selling photographs, the latter of which may qualify such an entity as a covered entity. There is a definition of journalism, and one wonders if companies like Facebook or Google will try to get some of their activities exempted on the basis that they qualify as journalism.

The Act adds a section to the federal criminal code on extortion and threats titled "Disclosure of personal information with the intent to cause harm," that makes a criminal offense of the actual or attempted disclosure of personal information to threaten, intimidate, or harass another person in order to commit or incite an act of violence. It is also a criminal offense to do so if a person is placed in reasonable fear of death or serious bodily injury. Violators would face fines and prison sentences

of up to five years in addition to any state liability as this would seem to cover a number of crimes ushered in by the digital age: doxing, revenge porn, or making public a person's private information in order to intimidate.

Title I of the "Online Privacy Act of 2019" would provide individuals with a number of rights regarding their personal information and how it may and may not be used by covered entities. First, people would receive a right of access which entails each covered entity making available a reasonable mechanism by which a person find out the categories of personal information and contents of communications being held and those obtained from third parties. Moreover, this information must also contain all the third parties, subsidiaries, and affiliates to whom personal information has been disclosed. Also, individuals must be able to easily access a clear and concise description of the commercial and businesses purposes for which the covered entity collects, maintains, processes, and discloses personal information. Finally, covered entities must provide a list of all automated decision-making processes it employs and those a person may ask that a human being make instead of the automated processes. Covered entities may sidestep a number of these requirements by making it publicly available on its website in a conspicuous location obviating the need for people to make requests.

Individuals would also get a right of correction allowing for the use of a reasonable mechanism to dispute the accuracy and completeness of personal information being held by a covered entity, but only if this personal information is processed such fashion as to "increase reasonably foreseeable significant privacy harms." This language suggests that data processing that would result in mere privacy harms, say those that would impact one's personal, familial communications, would not need to be corrected or completed. In any event, covered entities have the option to correct or complete as requested, tell the requester the information is complete or correct, respond that insufficient information does not allow for the correction or completion, or deny the request on the basis of exemptions discussed below. Small businesses are exempted from this responsibility. Of course, what ultimately is determined to be a significant privacy harm will be the result of case-by-case adjudication by the new DPA, likely in court.

People could ask that their personal information be deleted, including those data acquired from third parties or inferred by the covered entity. Again, on the basis of Section 109 exemptions, this request could be denied.

Individuals will receive a right of portability, and in order to effectuate this right, the DPA must annually publish in the *Federal Register* categories of online services and products that are determined to be portable. However, before a final list is published, the DPA must release an initial list of portable services and products and accept comments. Once it has been established which services and products are portable, then covered entities must allow individuals to request and receive their personal information and/or contents of communications for purposes of taking their business to a competitor. There is also language that contemplates asking one covered entity to directly transmit this information on account of a person's request.

Upon request, covered entities must have humans make decisions instead of an "automated processing of personal information of an individual, if such processing increases reasonably foreseeable significant privacy harms for such individual."

Before a covered entity may engage in behavior personalization, it must obtain express, affirmative consent from a person to collect, process, maintain or disclose personal information for

this purpose. Behavior personalization is a term defined in the Act and "means the processing of an individual's personal information, using an algorithm, model, or other means built using that individual's personal information collected over a period of time, or an aggregate of the personal information of one or more similarly situated individuals and designed to—

- alter, influence, guide, or predict an individual's behavior;
- tailor or personalize a product or service; or
- filter, sort, limit, promote, display or otherwise differentiate between specific content or categories of content that would otherwise be accessible to the individual."

This right seems squarely aimed at the use of one's data to show him advertising based on their browsing history, searches, location, occupation, and the huge volumes of other data collected daily. Moreover, if a person denies such consent, then the product or service must be provided without the behavior personalization unless this is infeasible at which point only the core service or product need be provided. And, if it is infeasible to provide core services or products, then a covered entity may altogether deny a product or service. It is likely covered entities will seek to define "infeasible" as broadly as possible in order to leverage consent for its products and services and so that it may continue the lucrative practice of personalized advertising.

A person would also get the right to be informed which entails any covered entity that begins collecting personal information on a person despite there not being a direct relationship, the covered entity must inform the person within 30 days by writing.

There would be established a right to impermanence that would limit the holding a person's personal information for no more time than she consented to. Covered entities must obtain affirmative, express consent from people for categories of personal information for as long as the original purpose for collection is completed or by a certain date. And yet, there is an exemption for implied consent when long-term maintenance of personal information is an obvious, core feature of a product or service and these data are maintained only to provide the product or service.

As mentioned, Section 109 details the exemptions that may allow a covered entity to disregard the rights bestowed on people under the "Online Privacy Act of 2019," which include

- Detecting, responding to, or preventing security incidents or threats.
- Protecting against malicious, deceptive, fraudulent, or illegal activity.
- Complying with specific law enforcement requests or court orders.
- Protecting a legally recognized privilege or other legal right.
- Protecting public safety.
- Collection, processing, or maintenance by an employer pursuant to an employer-employee relationship of records about employees or employment status, except—
    - where the information would not be reasonably expected to be collected in the context of an employee's regular duties; or
    - was disclosed to the employer by a third party.
- Preventing prospective abuses of a service by an individual whose account has been previously terminated.
- Routing a communication through a communications network or resolving the location of a host or client on a communications network.
- Providing transparency in advertising or origination of user generated content.

However, the covered entity will need to have "technical safeguards and business processes that limit the collection, processing, maintaining, or disclosure of such personal information" to the aforementioned purposes.

This section also details the reasons why a covered entity may decline a request made pursuant to one of the rights listed in Title I:

- A requester's identity cannot be confirmed
- If the request would create a legitimate risk to the privacy, security, safety, or other rights of another person
- A legitimate risk to free expression
- In regard to completing or deleting requests, if doing so would stop a transaction or process set into motion but not completed per a person's request or such a request would undermine the integrity of a legally significant transaction

Service providers are altogether exempted from Title I, and covered entities employing privacy preserving computing are exempted from certain rights of people: right of access, right to human review of automated decisions, right of human review, and the right to individual autonomy. However, this exemption applies only to the data processing performed with privacy preserving computing.

Covered entities must reply to requests within 30 days and may not normally charge a fee for fulfilling requests unless it is determined that the requests are excessive or unfounded, then a covered entity may charge a fee subject to DPA approval.

Title II of the "Online Privacy Act of 2019" details the requirements placed on covered entities, service providers and third parties.

Covered entities must have a reasonable articulable basis for collecting, processing, maintaining, and disclosing personal information related to the reasonable business needs of the entity. Additionally, the covered entity must keep no more personal information than is necessary to effectuate the business or commercial purpose and these needs are to be balanced against privacy intrusions, possible privacy harms, and the reasonable expectations of people whose information in question. Additionally, covered entities should not collect more personal information than is necessary to carry out its business purpose nor should it hold these data longer than necessary. However, covered entities may engage in "ancillary" collection, processing, maintenance, and disclosure of personal information in certain circumstances subject to certain requirements. For example, if these activities are substantially similar to the original ones and it is the same type of personal information being collected and no privacy harms would result, then notice and consent are not required. However, notice is required for ancillary activities if:

- The ancillary activities the covered entity is engaged in are similar to the original activities and there is a privacy harm risk
- The ancillary activities are not substantially similar and there is not risk of privacy harms; or
- The activities are substantially similar and would result in privacy harm but privacy preserving computing is used

Consequently, notice and consent would be required for any other ancillary activities that do not fall into those categories.

Covered entities would also need to limit the access of employees and contractors to personal information and the contents of communication on the basis of an articulable rationale that balances reasonable business needs, the potential for privacy harm, and the reasonable expectations of individuals. Moreover, covered entities must maintain records on all access.

There is a requirement that covered entities cannot collect or maintain any personal information unless they are in compliance with the Act. However, this requirement does not cover processing or maintaining personal information.

The disclosure of personal information by covered entities to third parties is limited only to situations when a person consents. And, any such consent is only valid after a person has been notified of all the categories of third parties the personal information may be disclosed to, the personal information to be shared, and the business purposes for doing so. Sales of personal information would be more severely constrained. Each sale to a third party by a covered entity must be agreed to by a person. What's more, covered entities must disclose the parameters of the original purpose for the collection of the information when it sells it to a third party. Regarding the use of privacy preserving computing and de-identified personal information, disclosure does not require consent for either designation, but consent is always required for the sales of personal information.

There are provisions designed to sweep into U.S. jurisdiction players in the data ecosystem that are outside the country. The bill bars covered entities from disclosing personal information to entities not subject to U.S. jurisdiction or not in compliance with the Act. However, a safe harbor is created under which covered entities and non-U.S. entities could do business that is largely premised on the latter being willing to comply with the Act, having the cash available to pay fines for violations, and evince a willingness to be subject to DPA enforcement. The non-U.S. entity also needs to sign an agreement with the DPA. This section, however, makes clear it is seeking to create a data localization requirement in the U.S or to restrict a covered entity's internal disclosures, so that Microsoft, say, could continue shuttling personal data around the globe to its servers without running afoul of this section.

Covered entities are barred from re-identifying de-identified information unless allowed by one of the Section 109 exemptions, and this prohibition attaches to third parties that may have the de-identified information. However, "qualified research entities" are not covered by this restriction, and it would be up to the DPA to determine who may be considered one.

A covered entity's ability to collect, process, maintain, or disclose the contents of communication would be limited only to those situations where there is a security incident or threat, the processing is expressly requested by one of the parties to the communication, and other specified purposes. There is an exception for publicly available communications, and covered entities cannot stop people using their services or products from encrypting their communications. There is a safe harbor for service providers acting at the direction of a covered entity with a reasonable belief the directions comply with the Act.

Covered entities could not process personal information in a way that impinges a person's opportunities on the basis of a protected class in education, employment, housing, credit, healthcare, finance, and a range of other areas. The same is true of public accommodations. Moreover, the DPA is required to promulgate regulations to effectuate this section.

The use of genetic information would be very severely limited, and more or less these types of data would only be available for medical testing and even then, subject to restrictions.

The DPA will establish a minimum percentage threshold for people to read and understand a notice for purposes of consent or a privacy policy that covered entities would need to meet or exceed before its notice or privacy policies would be allowed to be used. The DPA will establish a procedure to vet the data submitted by covered entities to show compliance with this requirement. Moreover, the DPA will make available the notices and privacy policies of all covered entities. All covered entities must make available reasonable mechanisms for people to revoke consent. And, not surprisingly, deceptive notices and privacy policies are barred.

Pursuant to these DPA approved notices, covered entities must provide clear and concise notice of the personal information being collected, maintained, processed, or disclosed. Additionally, covered entities may not collect, process, maintain, or disclose personal information without consent if it creates or increases the risk of foreseeable privacy harms. However, consent will be implied if the personal information activities of an entity are obvious on their face and notice is provided. However, privacy preserving computing would be exempt from the notice and consent requirements.

Covered entities shall, of course, have privacy policies regarding tis personal information activities, including a general description of its practices, an explanation as to how individuals may exercise their Title I rights, the categories of personal information collected, the business or commercial purposes for which such data will be used, and other requirements.

Information security would be a part of the new regime covered entities must comply with. Consequently, covered entities must design and establish an information security system to protect personal information based on the sensitivity of the data and the types of activities in which the covered entity is engaged. The information security system must include

- A written security policy
- A means of identifying, assessing, and mitigation security vulnerabilities
- A process for disposing personal information securely
- A process for overseeing those with access to personal information; and
- A plan or protocol to respond to data breaches or data sharing abuses

In the event a data breach or data sharing abuse occurs, the covered entities must report it to the DPA within 72 hours of discovery unless the event is unlikely to create or increase foreseeable privacy harms. Any notifications made after this 72-hour window must be accompanied by reasons why it was delayed. Additionally, a covered entity must alert other covered entities from whom they personal information, and people must be notified if there is a risk of increased privacy harms.

Title III details the DPA's structure and powers. The DPA would be headed by a Director appointed by the President and confirmed by the Senate, and the Director could appoint a Deputy Director. The Director would serve a five year, and the bill is silent is on how many terms a Director may serve. The agency would receive broad powers to set itself up and to promulgate regulations for its operations or to regulate entities under its jurisdictions. The DPA must consult with other federal agencies and state agencies in policing privacy and security. Finally, the agency would have appropriations of $550 million per year for the next five years authorized, but the Appropriations Committees would have to actually make these funds available in annually in an appropriations bill.

Title IV lays out the enforcement of the Act. The DPA could enforce the Act in two separate ways, much like the FTC's current means of enforcement. It could initiate an internal, administrative process that would result in a cease and desist order, allowing any such defendant in this action the opportunity to challenge the agency at an agency hearing and then appealing from what would presumably be an administrative law judge's decision to the full agency, and then to a U.S. Circuit Court of Appeals. Or, the DPA could file a complaint in a U.S. District Court and litigate against a defendant. In either case, the agency could seek civil penalties of up to $42,530 per person, and this number could get high depending on the number of people involved. For example, in the Facebook/Cambridge Analytica case where more than 87 million people were affected, if the DPA sought the maximum civil fine for each violation, the potential liability would be more than $37 trillion. It is important to note that civil penalties are calculated per person and not per violation, for the latter method could yield even larger numbers as it is easy to contemplate multiple violations per person. However, a court's directions under the Act in terms of the factors to consider when meting out a fine would weigh against such a gigantic, company crushing fine.

In enforcing the act, the DPA must coordinate with other federal regulators, which means multiple, overlapping jurisdictions is the likely future landscape is this bill is enacted. These agencies may refer cases to the DPA for prosecution, and yet, should one federal agency initiate an action for a privacy or security violation, the DPA may not also bring an action. Moreover, the Act requires the DPA to execute an agreement with the FTC to coordinate enforcement. State attorneys general may bring actions under this Act but only if the DPA is not doing so, and the state needs to provide notice to the DPA before proceeding.

As noted, a private right of action is available for people to allege violations of the Act. However, a class action seeking civil damages could only be brought by a non-profit and not plaintiffs' attorneys, suggesting a class action for injunctive relief may be brought by a plaintiffs' attorney. There is also a provision allowing a whistleblower to bring an action after first allowing the DPA the option to litigate. If the DPA accepts and prevails, the whistleblower would be entitled to 15%, but if the whistleblower litigates the case, she may be entitled to between $25 and 50% of the award.

In terms of the relief the DPA or a state attorney may recover aside from civil penalties, a range of equitable relief:

- Rescission or reformation of contracts;
- Refund of moneys;
- Restitution;
- Disgorgement or compensation for unjust enrichment;
- Payment of damages or other monetary relief;
- Public notification regarding the violation, including the costs of notification; and
- Limits on the activities or functions of the person;

Additionally, the DPA or state attorneys general may also seek to recover all the costs of prosecuting the case.

AI Commission's Interim Report

The National Security Commission on Artificial Intelligence (AI) has released its interim report and explained that "[b]etween now and the publication of our final report, the Commission will pursue answers to hard problems, develop concrete recommendations on "methods and means" to integrate

AI into national security missions, and make itself available to Congress and the executive branch to inform evidence-based decisions about resources, policy, and strategy." Former Google Chair Eric Schmidt serves as the Commission's chair, and former Deputy Secretary of Defense Robert Work is the vice chair, and there are 13 other commissioners. The Commission released its initial report in July that laid out its work plan.

The Commission claimed that the interim report "fulfills Congress's request for the Commission's preliminary assessment of these challenges and opportunities." The Commission contended that "[i]t is an attempt to inform policy and public debate about how developments in AI are related to wider national security trends." The Commission added that "[w]e are not yet in a position to make final recommendations, suggest major organizational changes, or propose specific investment priorities in rank order attached to dollar figures." The Commission expressed its belief "that laying out the basic fundamentals, presenting some consensus guiding principles, and offering initial preliminary judgments will contribute to public debate as the Commission moves toward its final report." The Commission "developed seven consensus principles to guide our work and national discussion:

- First, global leadership in AI technology is a national security priority. The U.S. government retains a core responsibility to steer advancements in ways that protect the American people and ensure a robust basic research environment.
- Second, AI adoption for national security is an urgent imperative. We see no way to protect the American people, U.S. interests, and shape the development of international norms for using AI if the United States is not leading the way in application.
- Third, private sector leaders and government officials must build a shared sense of responsibility for the welfare and security of the American people. The government needs help from industry and academia to maximize the promise of AI and minimize the national security risks posed by AI.
- Fourth, people matter more than ever in the AI competition: we must cultivate homegrown AI talent and continue to attract the world's best minds.
- Fifth, actions taken to protect America's AI leadership from foreign threats must preserve principles of free inquiry, free enterprise, and the free flow of ideas.
- Sixth, at a basic level we see a convergence of interests and concerns between national security officials and those in the AI development and ethics community. Everyone wants safe, robust, and reliable AI systems; at the same time, today's technical limitations are widely recognized. Disagreements will persist, but we believe there is common ground that can serve as the basis for productive conversations.
- Seventh, any use of AI by the United States must have American values—including the rule of law—at its core.

The Commission "identifies five fundamental lines of effort that are necessary to preserve U.S. advantages:

- *Invest in AI Research and Development (R&D);*
    - Federal R&D funding for AI has not kept pace with the revolutionary potential it holds or with aggressive investments by competitors. Investments that are multiple times greater than current levels are needed.
    - Untapped opportunities exist to build a nationwide AI R&D infrastructure and encourage regional innovation "clusters." Such AI districts for defense would benefit both national security and economic competitiveness.
    - The U.S. government should implement more flexible funding mechanisms to support AI research. Business as usual is insufficient.

    - The U.S. government must identify, prioritize, coordinate and urgently implement national security-focused AI R&D investments.
    - Bureaucratic and resource constraints are hindering government-affiliated labs and research centers from reaching their full potential in AI R&D.
- *Apply AI to National Security Missions;*
    - AI can help the United States execute core national security missions, if we let it.
    - Implementation of the government's security strategies for AI is threatened by bureaucratic impediments and inertia. Defense and intelligence agencies must urgently accelerate their efforts.
    - Pockets of successful bottom-up innovation exist across DOD and the IC. These isolated programs cannot translate into strategic change without top-down leadership to overcome organizational barriers.
    - AI adoption and deployment requires a different approach to acquisition.
    - Rapidly fielding AI is an operational necessity. To get there requires investment in resilient, robust, reliable, and secure AI systems.
    - AI is only as good as the infrastructure behind it. Within DOD in particular this infrastructure is severely underdeveloped.
    - The U.S. government is not adequately leveraging basic commercial AI to improve business practices and save taxpayer dollars. Departments and agencies must modernize to become more effective and cost-efficient.
- *Train and Recruit AI Talent;*
    - National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools.
    - DOD and the IC are failing to capitalize on existing technical talent because they do not have effective ways to identify AI-relevant skills already present in their workforce. They should systematically measure and incentivize the development of those skills.
    - The U.S. government is not fully utilizing civilian hiring authorities to recruit AI talent. Agencies need to make better use of pipelines for people with STEM training.
    - Expanding AI-focused fellowships and exchange opportunities can give officials and service members access to cutting-edge technology, and bring talent from our top AI companies into federal service.
    - The military and national security agencies are struggling to compete for top AI talent. They need a better pitch, incentive structure, and better on-ramps for recent graduates.
    - Two realities about the American AI talent pool have become clear to us:
        - 1. Colleges and universities cannot meet the demand for undergraduate student interest in AI and computer science generally.
        - 2. The American AI talent pool depends heavily on international students and workers. Our global competitiveness hinges on our ability to attract and retain top minds from around the world.
- *Protect and Build Upon U.S. Technology Advantages;*
    - The U.S. government should continue to use export controls—including multilateral controls—to protect specific U.S. and allied AI hardware advantages, in particular those in semiconductor manufacturing equipment.

    - Traditional item-based export controls and narrowly-scoped foreign investment reviews are by themselves insufficient to sustain U.S. competitiveness in AI.
    - The United States must continue leading in AI-related hardware, and ensure the government has trusted access to the latest technologies.
    - Law enforcement and academic leaders can and should find common ground on preserving an open research system while reducing security risks from foreign government-directed activity on American campuses.
- *Marshal Global AI Cooperation.*
    - The United States must enhance its competitiveness in AI by establishing a network of partners dedicated to AI data sharing, R&D coordination, capacity building, and talent exchanges.
    - AI presents significant challenges for military interoperability. If the United States and its allies do not coordinate early and often on AI-enabled capabilities, the effectiveness of our military coalitions will suffer.
    - U.S. diplomacy should be open to possible cooperation with China and Russia on promoting AI safety and managing AI's impact on strategic stability.
    - The United States should lead in establishing a positive agenda for cooperation with all nations on AI advances that promise to benefit humanity.

This commission was created by the FY 2019 National Defense Authorization Act (NDAA) (P.L. 115-232), and it noted its "broad mandate to examine AI through the lens of national competitiveness, the means to sustain technological advantage, trends in international cooperation and competitiveness, ways to foster greater investment in basic and advanced research, workforce and training, potential risks of military use, ethical concerns, establishment of data standards, and the future evolution of AI." The above initial recommendations would seem to call for a marshaling and commitment of national resources on the order of the Moon Race, and it is not yet clear if Congress and the White House have the appetite or willingness to commit the kinds of multi-billion dollar resources these recommendations seemingly call for.

The Commission, of course, did touch on the role China's push to develop AI plays in an appropriate and effective U.S. approach. The Commission contextualized the AI "revolution" as part of the "reemergence of great power competition." The Commission noted the many national plans on AI other nations have published but singled out China as "our most serious strategic competitor" to the U.S. that "has declared its intent to become the world leader in AI by 2030 as part of a broader strategy that will challenge America's military and economic position in Asia and beyond." Among the threats posed by AI that the Commission identified and discussed, China was named as being part of the issue in two: erosion of U.S. military advantage and erosion of civil liberties and privacy. The People's Republic of China (PRC) was cited as a strategic competitor likely to explore and implement AI as a means to negate and overcome current U.S. military advantages. Additionally, Russia was also mentioned as a related threat. Regarding civil liberties and privacy, the Commission seems to be extrapolating from current non-AI surveillance and oppressive practices in China to conclude reasonably that the further development of AI will aid the regime in Beijing in achieving these goals. In fact, the Commission cited China as being among 75 countries currently deploying "AI-powered surveillance." AI was also discussed in the context of current efforts by China to obtain U.S. technology by virtually any means, and the Commission asserted its judgment that any U.S. AI advances would fall prey to similar efforts.

The Commission detailed the intertwined nature of the U.S.-China technology relationship in a section titled "The China Entanglement Challenge." The Commission asserts "China represents the most

complex strategic challenge confronting the United States because of the many co-dependencies and entanglements between the two competitors." The Commission stated that "[g]iven the current trade tension, on top of a broader and growing global competition, many wonder if the United States should disentangle its economy and research network from China—including in the deeply interconnected field of AI." The Commission explained:

> The Commission is seeking to better understand the specific actions that will balance competing interests and chart a sensible path forward for preserving beneficial elements of cooperation while establishing defenses against activities that run counter to American interests. The challenge the United States faces is how to recalibrate elements of the U.S.-China tech relationship to be more conducive to American interests and preserve U.S. advantages, taking into account realistic assessments of Chinese state-directed behavior, the need to mitigate intellectual property theft, and the importance of preventing the proliferation of technology used for human rights abuses.

The Commission noted a number of "Trendlines of Concern," and not surprisingly China was named in each one:

- Research and Development: China has overseen a 30 times increase in its overall R&D funding from 1991 to 2015, and is projected to surpass the United States in absolute R&D spending within 10 years. U.S. federal investment in AI R&D has increased only marginally, as we discuss in greater detail below. Incrementalism will not assure U.S. leadership. America's leadership in AI research—measured by indicators such as academic publications—is also shrinking. For example, one study found that Chinese researchers are "poised to overtake [their American counterparts] . . . in the most-cited 10% of papers next year, and in the 1% of most-cited papers by 2025."
- Commercial Competition: Chinese tech firms have reached enormous scale and are poised to become leaders in applied AI, excelling in numerous commercial AI applications, including in healthcare, education, and e-commerce. Some of these applications may pose national security risks. China's new "national team" of leading Chinese tech firms (including Baidu, Alibaba, Tencent, iFlytek, and Sensetime) is being harnessed to promote national objectives in AI, including by supporting national laboratories working on deep learning, brain-inspired intelligence, and virtual/augmented reality. The global reach and sophistication of these companies may soon eclipse American counterparts, giving Chinese firms access to the data, resources, and market power required to lead in AI.
- Military-Civil Fusion: China is intensifying efforts to exploit civilian and commercial developments in AI and leveraging a growing number of companies to advance Party-state and military purposes. The Chinese Communist Party's concept of "military-civil fusion" has been elevated in national strategies and advanced through a range of initiatives. The distinction between civilian and military-relevant AI R&D is being eroded.
- Military Modernization: China and Russia each have established research and development institutes to advance their military applications of AI, akin to the Defense Advanced Research Projects Agency (DARPA). Chinese researchers are developing military applications of AI technologies—including for swarming, decision support, and information operations—while the Chinese defense industry is pursuing the development of increasingly autonomous weapons systems. China is pursuing a process of "intelligentization" as a new imperative in military modernization.
- Global Talent: The United States is facing new competition for global STEM talent, especially in AI where there is a critical shortage of expertise. China is undertaking an active effort to recruit global AI talent and persuade Chinese nationals working abroad to return

to China. Other countries are introducing favorable immigration and work policies to attract AI talent. We are beginning to see troublesome signs that America's ability to attract and keep the top global talent may be weakening.

Senate Judiciary Considers FISA Reauthorization

Ahead of the December 15, 2019 expiration of four surveillance provisions in the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015," (USA FREEDOM Act) (P.L. 114-23), the Senate Judiciary Committee held a hearing on these provisions. The expiring parts of the Foreign Intelligence Surveillance Act (FISA) in question are the 1) call detail records provisions; 2) roving wiretap authority; 3) the lone wolf provision; and the 4) business records provisions, and the Trump Administration is asking that Congress *permanently* extend these programs instead of reauthorize 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."

Reauthorization is considered must-pass and may figure in the coming end-of-the-year log jam of legislation that may include an extension of the current continuing resolution to fund the government in FY 2020 and articles of impeachment against President Donald Trump. Additionally, the House Intelligence and Judiciary Committees may be preoccupied with the latter matter and may have limited resources and bandwidth to address these FISA provisions. However, there is significant opposition to reauthorizing the authority that has allowed the National Security Agency to query databases of call records, and in a September hearing, House Judiciary Committee Chair Jerrod Nadler (D-NY) said the Administration will need to make the case for reauthorization beyond possibly needing these authorities in the future.

Chair Lindsey Graham (R-SC) said that there are four parts of the "USA FREEDOM Act of 2015," and he wants the witnesses to tell us "the good, the bad, and the ugly" and "why we need these four tools." He also wanted to know why reauthorization these programs is important, what happens if the Congress does not reauthorize these programs, and what, if any, changes the witnesses would like to see. Graham said he also wanted to hear from a national security perspective why the statute is still relevant in 2019 and beyond. He stated he wanted to know about the tools available to law enforcement under the statute and how they are relevant to the "fight we're still in." Graham declared that Baghdadi is dead the cause still lives, and the effort to penetrate the U.S. is ongoing every day. He claimed that terrorist groups "with a lot of different names are trying to come here to do us a lot of harm and to hurt Americans abroad." Graham contended that "the war is far from over" and there are no armed forces to defeat or capitals to conquer. He claimed that those "who embrace this ideology embrace death, and the only way to protect America is to hit them before they hit you." Graham stated that it is imperative to stop "them over there before they get here, and the only way to do that is to find out what they're up to using acceptable tools within our Constitutional democracy."

Ranking Member Dianne Feinstein (D-CA) said the hearing allows for a close look at provisions of the "USA FREEDOM Act of 2015" that are set to expire on December 15, 2019, including Section 215, otherwise known as the business records provision, as well as roving wiretap authority, and the lone wolf provision. She noted the committee played a key role in establishing and modifying

these authorities, so it is important to weigh in from time to time on any legislative changes that may be needed. Feinstein said she wanted to focus on Section 215 which requires third parties such as phone companies to produce business records. She asserted that Section 215 was used by the National Security Agency to conceal "hundreds of millions of domestic phone records." Feinstein stated that Congress prohibited this bulk collection in the "USA FREEDOM Act of 2015" introduced by Senators Pat Leahy (D-VT) and Mike Lee (R-UT). She stated that instead of bulk collection by the government, records remain with phone providers and are searchable only with a FISA order for "specific selection term," and that is generally a specific phone number or address. She said that this call detail record (CDR) is meant to ensure that surveillance is sufficiently targeted, but in June 2018, NSA publicly announced that due to technical irregularities, the CDR program had received data it was not legally authorized to receive. Feinstein noted the agency could no longer distinguish between records that were obtained lawfully and those that were obtained unlawfully. She stated that NSA subsequently announced it would delete all CDR acquired over the last three years. Feinstein stated that in August, the Director of National Intelligence Dan Coats confirmed that NSA had suspended the CDR program indefinitely due to its lack of intelligence value as well as its cost and compliance issues. Feinstein said that despite this, the Trump Administration is asking Congress to permanently authorize this program. She explained that it was not clear to her why a program with limited intelligence value and clear compliance problems should be reauthorized. Feinstein said that unless there is good reason to believe that it should, she does not believe it should be reauthorized.

Deputy Assistant Attorney General Brad Wiegmann, Federal Bureau of Investigation Deputy Assistant Director for the Counterterrorism Division Michael Orlando, and National Security Agency official Susan Morgan stated:

- Three of the authorities – the roving wiretap, business records, and lone wolf provisions -- have been part of FISA for well over a decade and have been renewed by Congress multiple times, most recently in the USA FREEDOM Act of 2015 (FREEDOM Act). Before that, these same authorities were reauthorized multiple times between 2005 and 2011, each time following extensive congressional review and deliberation. Each renewal gained bipartisan support.
- As this Committee is aware, the NSA recently discontinued the CDR program for technical and operational reasons. But the CDR program retains the potential to be a source of valuable foreign intelligence information. The CDR program may be needed again in the future, should circumstances change. NSA's careful approach to the program, and the legal obligations imposed by the FREEDOM Act in the form of judicial oversight, legislative oversight, and transparency, support the reauthorization of the CDR program.
- We urge the Committee to consider permanently reauthorizing these authorities based not only on the Government's demonstrated record and the importance of the authorities to national security, but also on the significant reforms contained in the FREEDOM Act. These include authorizing the FISC to appoint *amici curiae* to address privacy and civil liberties concerns and enhancing public transparency and reporting requirements under FISA. Four years ago, the FREEDOM Act was passed after extensive oversight and comprehensive hearings, and received strong bipartisan support in the Senate. In the wake of repeated reviews and bipartisan authorizations over nearly two decades, the Administration's view is that the time has come for Congress to extend these authorities permanently.
- The roving wiretap authority has proven to be an important intelligence-gathering tool. The Government has used the authority in a relatively small number of cases each year. Those cases tend to involve highly-trained foreign intelligence officers operating within the United States, or other important investigative targets, including terrorism-related targets, who

have shown a propensity to engage in activities deliberately designed to thwart surveillance. Similar authority designed to prevent suspects from thwarting surveillance has been a permanent part of our criminal law for over thirty years, and this provision has been renewed as part of FISA repeatedly since 2001 without controversy or evidence of abuse. It remains an important tool, and we strongly support permanent reauthorization.

- Second, we also support permanent reauthorization of the so-called "business records" provision, which was enacted as section 215 of the USA PATRIOT Act in 2001. This provision authorizes the Government to apply to the FISC for an order directing the production of business records or other tangible things that are relevant to an authorized national security investigation. It allows the Government to obtain in a national security investigation many of the same types of records and other tangible things that the Government can obtain through a grand jury subpoena in an ordinary criminal investigation. The Government has used the business records provision to obtain, for example, driver's license records, hotel records, car rental records, apartment leasing records, and the like.
- Some criticize the business records provisions as running afoul of the Fourth Amendment because business records orders are not issued under a "probable cause" standard. But an order issued under the business records provision does not authorize the Government to enter premises, or to search for or seize records or other tangible things. Thus, the Fourth Amendment's probable cause standard generally does not apply. Rather, the records the Government is authorized to obtain—pursuant to a FISC order—are similar to those that the Government could obtain in ordinary criminal or civil investigations—without *any* court order in most instances— pursuant to a grand jury subpoena in an ordinary criminal case, or pursuant to an administrative subpoena in a civil case. Like a grand jury subpoena or an administrative subpoena, a business records order merely requires the recipient to identify and produce responsive records or other tangible things.
- To be sure, this authority has generated substantial controversy because it was employed, with FISC approval, to support NSA's bulk telephony metadata collection program. However, that program has been terminated and replaced by the more targeted collection of telephony metadata authorized under the CDR provisions of the FREEDOM Act, as discussed below. The FREEDOM Act permanently banned bulk collection altogether under the business records authority and required the use of a "specific selection term" to justify an application for a business records order.
- The Government has used the business records authority judiciously. On average, between 2015 and 2018, the Government sought and obtained records under this provision less than 76 times per year. The number of business records applications approved has decreased every year since 2012. Many of these investigations involve scenarios that are outside the scope of the National Security Letter statutes, and often a business records order is sought because national security interests preclude the use of less secure criminal authorities, or because there may be no criminal investigation underway. Given the importance of the authority, the absence of any evidence of abuse, and the additional safeguards Congress imposed in 2015, we urge the Committee to support permanent reauthorization of this provision.
- The third expiring provision is the so-called "lone wolf" provision of FISA. It allows the FISC to authorize surveillance of *non-United States persons* engaged in international terrorism or the international proliferation of weapons of mass destruction, without the need to show that the target is acting on behalf of a particular terrorist group or other foreign power.
- Although the Government has not used the lone wolf authority to date, it fills an important gap in the Government's collection capabilities. The provision allows for the surveillance of a foreign terrorist who might be *inspired by* a foreign group, but who is not technically an

agent of that group. For example, the provision would allow for surveillance of a foreign person who has self- radicalized through internet propaganda of a foreign terrorist organization, or a known international terrorist who severs his connection with a terrorist group. The Government's decision not to employ this authority to date does not mean that it should be abandoned. To the contrary, it shows that the Government will use this provision only where necessary and legally available. Terrorist groups like ISIS and al-Qaida actively seek to encourage lone wolf attacks. The continued availability of the lone wolf provision ensures the Government retains the authority to surveil isolated foreign terrorist actors who are inspired, but not directed by, foreign terrorist groups.

- Finally, as we have explained, in addition to reauthorizing these longstanding provisions of FISA in 2015, the FREEDOM Act banned bulk collection and established a new, narrowly-tailored mechanism for the targeted collection of CDRs from U.S. telecommunications service providers. The new provisions were enacted after comprehensive oversight, including hearings addressing recommendations of a presidentially-appointed group of outside experts and the Privacy and Civil Liberties Oversight Board, which weighed in on the privacy and civil liberties effects of the authorities and their importance to national security.

Privacy and Civil Liberties Oversight Board (PCLOB) Chair Adam Klein stated that "[i]n advance of this year's reauthorization deadline, our Board has reviewed NSA's collection of call detail records under the USA Freedom Act…[and] [r]ecently, we submitted a 116-page draft report to the Intelligence Community for classification review." He stated that "[t]he report contains a comprehensive account of the "technical" and "operational" issues cited in NSA's public statements…[and] also includes legal analysis, policy analysis, and the views of individual Board Members." Klein remarked that "[a]t present, the document remain sclassified, but I can provide a few top-line conclusions based on my knowledge of the facts that we found in our review." He declared that "[o]ur review found no malfeasance or abuse of this authority…[n]or did it find any instance in which government officials intentionally sought records that were prohibited under the statute." Klein stated that "[t]he Board found no evidence that NSA received any of the statutorily prohibited categories of information: no subscriber names or addresses, no financial information, no cell-site location information, no GPS coordinates."

Klein stated that "[w]e also examined the government's operational use of this program…[and] NSA chose to suspend the program after balancing its "relative intelligence value" against other factors." He said that "[b]ased on the facts we found, my view is that NSA's decision was well supported by the available evidence." Klein asserted that "[o]ur report also contains a comprehensive account of the "compliance and data integrity concerns" that led NSA to delete data and eventually influenced its decision to suspend the program." He stated that "[o]ur review of these facts confirmed that the data-integrity challenges the program encountered were inadvertent, not willful." Klein stated that "[w]hen NSA received records that raised questions about the scope of permitted collection under the statute, the agency chose to follow a narrower understanding of its authority under the USA Freedom Act, rather than a more expansive interpretation that would have given it greater leeway."

George Mason University's Antonin Scalia Law School Professor Jamil Jaffer asserted:

> If we look at the public record with respect to the challenges that NSA faced on Section 215 in mid-2018, it becomes clear that the challenge was less on NSA's end and more on the providers who were supplying the information to NSA under the USA FREEDOM Act. Specifically, at some point in early 2018, NSA analysts "noted technical irregularities in

> some data received from telecommunications service providers....[which]resulted in the production to NSA of some CDRs that NSA was not authorized to receive." And because NSA was unable to "identify and isolate properly produced data," NSA determined that it should not use any of the CDRs and decided, after consulting with DOJ and ODNI, to delete the data. Later descriptions of what followed, and what led to the ultimate decision to terminate the program are likewise instructive: the former DNI, in informing Congress of the Intelligence Community's view that the CDR program and other expiring authorities ought be renewed and made permanent, noted that a key factor informing whether to continue the CDR program was presence of "compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes." This statement appears to make clear that NSA was not only concerned that the data being provided by the carriers may not have met the legal requirements but also that the data itself may not have been valid for use in intelligence investigations, and that this problem arose in part because of the use of company-generated data.

Jaffer stated

> If this reading of the historical record is correct, then one might wonder whether NSA would have been able to more effectively correct the data issues going forward—as it had done a number of times before when confronted with compliance issues—had it not been mandated, by statute, to not collect and house the data itself. Given this open question—as well the unanimous view of the intelligence professionals before the Committee today that this program ought be reauthorized—Committee may wish to consider providing NSA and ODNI with options under which they might restart the program and provide potential pilot opportunities for NSA to explore how it might collect data in a way that avoids these problems.

Jaffer stated that "[t]he Committee may wish to consider the following options and potential reforms as it looks to act in the near future on reauthorization of the expiring authorities:

> 1.With respect to the CDR program, the Committee may wish to consider retaining the existing authority and structure for the program, while requiring NSA to report back to Congress before it restarts the program and to provide the Committee with a detailed explanation of how it intends to meet the statutory requirements going forward.
> 2. The Committee may also wish to permit NSA to run a short-term pilot CDR program where it once again takes on its pre-USA FREEDOM role of holding a significant subset of the data it needs to do its work—perhaps in a new technology area—to see whether taking on the data itself allows NSA to mitigate the compliance and data integrity issues it experienced under the carrier-based system required by the USA FREEDOM Act.
> 3. With respect to additional transparency measures, the Committee might consider requiring the FISC to publish a classified and unclassified reporter of all of its opinions, with the latter version redacted to protect sources and methods of intelligence collection, as well as information about the targets of collection, in consultation with the Office of the Director of National Intelligence. Such a reporter would serve to better inform government officials, the government and private sector legal community, and the public about the work of the court and the legal analysis it applies to the issues that come before it in both the classified and unclassified settings.
> 4. In order to address potential concerns about the ability of the judges of the FISC to operate independently and to keep up with the work of the court from their home districts, the Committee may wish to consider providing the judges of the FISC with direct, regular

> access to opinions that are issued by their colleagues while in their home districts, either through access in a secure compartmented information facility at the local federal courthouse or at another appropriate government facility in the area.
> 5. In parallel, the Committee may also wish to consider providing resources to the Administrative Office of the U.S. Courts to ensure that each judge of the FISC has a fully-cleared, term law clerk to assist the judge with their FISA caseload, both while in their home districts as well as while in the Washington area for FISC hearings. If the Committee decides to undertake this reform, the Committee may wish to consider whether the FISC's legal advisors continue to be necessary.

New York University School of Law's Liberty and National Security Program Elizabeth Goitein stated that "the following reforms should accompany any reauthorization of Section 215 of the Patriot Act:

- End the call detail records program that replaced the NSA's "bulk collection" program
- Narrow "bulky" collection under other authorities
- Prohibit warrantless collection of geolocation and other particularly sensitive records
- Prohibit discriminatory surveillance or surveillance based on First Amendment-protected activities
- Establish meaningful minimization requirements
- Close the backdoor search loophole in Section 702 surveillance
- Strengthen transparency and oversight provisions

Goitein asserted that "Congress should also revisit the two other Patriot Act provisions that are scheduled to expire on December 15: the so-called "lone wolf" and "roving wiretap" provisions." She contended that "[t]he lone wolf provision should be allowed to sunset, as it is both unnecessary (it has never been used) and unwise (it jettisons a critical limiting principle in the application of FISA surveillance authority)…[and] [t]he roving wiretap provision should be amended so that it conforms to the parallel provision for criminal wiretaps."

T-Mobile Sprint Merger Approved at the Federal Level; State Challenge Ongoing

Last week, the Department of Justice (DOJ) and the Federal Communications Commission (FCC) greenlit the merger between the third and fourth largest wireless carriers in the U.S. even though a number of state attorneys general are suing to block the merger.

On November 8, the Department of Justice (DOJ) released its responses to comments on the proposed final judgment on the T-Mobile/Sprint merger. The DOJ claimed that

> the remedy the United States obtained addresses the competitive harm alleged in this action and is in the public interest. Accordingly, the United States recommends no modifications to the proposed Final Judgment. This remedy, now adopted by the Attorneys General of eight states who have joined this lawsuit and endorsed by two more through comments in this proceeding, promises to expand output in the mobile wireless market and be a boon for American consumers. The Federal Communications Commission has concluded that the proposed transaction, as modified by the FCC's own set of conditions, would be in the public interest. In reaching this conclusion, the FCC recognized the significant benefits that the proposed Final Judgment would yield. Commenters in this proceeding recognize these benefits as well—the United States received 32 comments regarding the settlement, the majority of which were supportive of the merger and/or the proposed Final Judgment.

The DOJ claimed that

> The proposed Final Judgment provides for a substantial divestiture which, when combined with the mobile wireless spectrum already owned by DISH Network Corp. ("DISH"), will enable DISH to enter the market as a new 5G mobile wireless services provider and a fourth nationwide facilities-based wireless carrier. T-Mobile and Sprint must divest to DISH Sprint's prepaid businesses, including more than 9 million Boost Mobile, Virgin Mobile, and Sprint-branded prepaid subscribers, and make available to DISH more than 400 employees currently running these businesses. The proposed settlement also provides for the divestiture of certain spectrum assets to DISH, and it requires T-Mobile and Sprint to make available to DISH at least 20,000 cell sites and hundreds of retail locations. T-Mobile must also provide DISH with robust access to the T-Mobile network for a period of seven years while DISH builds out its own 5G network.

DOJ claimed that

> The United States expects the proposed Final Judgment will provide substantial long-term benefits for American consumers by ensuring that large amounts of currently unused or underused spectrum are made available to American consumers in the form of advanced 5G networks that this proposed Final Judgment will help facilitate. Under commitments made to the FCC that have been incorporated into the proposed Final Judgment, DISH, which has been joined as a defendant in this action, is required to bring its existing spectrum resources online in a nationwide, greenfield 5G wireless network or risk substantial penalties at the FCC and in this Court. Under T-Mobile's commitments to the FCC, which are also incorporated into the proposed Final Judgment, the merged firm will combine T-Mobile's and Sprint's existing complementary spectrum resources and build out a 5G network to deliver network capacity that exceeds the sum of what either carrier could achieve on its own.

On November 5, a split Federal Communications Commission (FCC) "issued a Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification approving—with conditions—the transfer of control applications filed by T-Mobile and Sprint" according to its press release. The vote was 3-2 to approve the proposed merger with conditions that would offset some of the anti-competitive effects of the U.S.'s third and fourth largest wireless providers.

The FCC contended that it "found that the transaction will help close the digital divide and advance United States leadership in 5G, the next generation of wireless connectivity." The Commission asserted that "[s]pecifically, T-Mobile and Sprint have committed within three years to deploy 5G service to cover 97% of the American people, and within six years to reach 99% of all Americans…[including] deploying 5G service to cover 85% of rural Americans within three years and 90% of rural Americans within six years." The FCC added that "[t]he parties also pledged that within six years, 90% of Americans would have access to mobile service with speeds of at least 100 Mbps and 99% of Americans would have access to speeds of at least 50 Mbps." The FCC added that "[t]his includes two-thirds of rural Americans having access to mobile service with speeds of at least 100 Mbps, and 90% of rural Americans having access to speeds of at least 50 Mbps."

The FCC stated that it

> conditioned its approval of the transaction on the parties fulfilling these commitments. Compliance with these commitments will be verified by rigorous drive-testing, overseen by an independent third party and subject to Commission oversight, to ensure that the service Americans receive will be what the parties have promised. And in order to ensure that these commitments are met, the parties will be required to make payments that could reach over two billion dollars if they do not meet their commitments within six years. Moreover, the parties will be required to make additional payments until they have fulfilled their commitments.

In the Memorandum Opinion, the FCC claimed

- As the two smallest nationwide mobile service providers, T-Mobile and Sprint assert that their combination will enable the deployment of a world-leading 5G network with capabilities beyond those either could achieve alone. Although each company had independent 5G plans, they claim that on their own they lack the capability to deploy 5G as broadly and with as much capacity as the resulting combined company, New T-Mobile, would. They maintain that their combined scale will increase network efficiency and that Sprint's mid-band spectrum will complement T-Mobile's low-band spectrum, further increasing the quality of their combined network. T-Mobile and Sprint also claim that these and other synergies will enable the merged firm to compete more effectively against the market leaders, AT&T and Verizon Wireless, than could either firm individually. As a result, they argue, the transaction would not result in the lessening of competition often associated with consolidation between horizontal competitors.
- Expanding 5G access to all Americans will also enhance the benefits of 5G innovation for the overall United States economy and will support American technological leadership. The larger the United States' 5G user base, and the broader its nationwide coverage, the greater the opportunity for entrepreneurs and innovators. The network benefits of the T-Mobile/Sprint transaction will thus extend beyond mobile wireless services alone, to enhance the competitiveness of the United States' economy.

The FCC further contended that

> At the end of the day, we believe that it is likely, even without conditions, that these competitive benefits will outweigh pricing pressure in certain areas, such as rural markets, and in certain segments of the market, such as consumers who are primarily quality-conscious. However, we are not confident that this will be the case across the board. In particular, based on the record, we are concerned about the impact of an unconditioned transaction on consumers in densely-populated areas who are primarily concerned about cost. Accordingly, we require, as a condition of our approval, that the Applicants fulfill a series of commitments to address the potential for lost price competition, such as the divestiture of Boost Mobile. These conditions eliminate the concerns otherwise identified in our review. Among other requirements, the Applicants have committed that the divested Boost Mobile will have low-cost wholesale network access on terms superior to typical MVNOs, with the financial incentive to provide robust competition from the moment of divestiture, and with the ability to build its own facilities over time. We conclude that, as conditioned, the transaction would not substantially lessen competition,14and would be in the public interest.

In her dissenting statement, Commissioner Jessica Rosenworcel argued:

- The proposed tie-up of T-Mobile and Sprint will reduce competition. This merger will combine two of the four nationwide competitors in the wireless industry in the United States. As a result, three companies will control 99 percent of the wireless market. By any metric, this transaction will raise prices, lower quality, and slow innovation, just as we start to deploy the next-generation of wireless technology.
- We've all seen what happens when market concentration increases following a merger. A condensed airline industry brought us baggage fees and smaller seats, even as the price of fuel fell. A condensed pharmaceutical industry has led to a handful of drug companies raising the prices of lifesaving medications, taking advantage of those struggling with illness. There's no reason to think the mobile-phone industry will be different. Shrinking the number of national providers from four to three will hurt consumers, harm competition, and eliminate thousands of jobs. In deciding to overlook these harms, the Federal Communications Commission and the Department of Justice have been wooed by a few unenforceable concessions and hollow promises from the two companies involved.

Rosenworcel stated

- Moreover, the remedies the FCC and the Department of Justice design around these promises betray the free-market principles that for decades have made us the world's leader in wireless. Instead of promoting vigorous competition among providers, today's order justifies increased concentration by jerry-rigging a new provider dependent on the government dictating who sells what to whom and when. In addition, the agency retreats from nimbler and more decentralized approaches to spectrum management—like flexible use licenses and technology-neutral rules—that have served us so well in the past. To add insult to injury, it made these choices behind closed doors with a remarkable lack of transparency.
- Both the FCC and Department of Justice should know better than to think that tinkering around the edges of this deal can save it. Across our economy and across our geography, we are already struggling with the consequences of a seemingly never-ending wave of mergers and lax enforcement. So many of America's most pressing economic and political problems can be traced back to this kind of market consolidation. This includes dwindling opportunity in rural America as farmers struggle against agriculture conglomerates. It includes plunging rates of entrepreneurship as concentrated markets choke off small businesses. It includes falling wages as mergers reduce the need for employers to compete to keep their workers. And it includes income and wealth inequality that are higher than they've been in a hundred years.

In their complaint, the attorneys general of New York, California, Virginia, and other states claimed

> On April 29, 2018, T-Mobile and Sprint agreed to combine, a decision supported by their respective controlling shareholders, Deutsche Telekom AG, Deutsche Telekom Holding B.V., and Softbank Group Corp. The proposed transaction would eliminate Sprint as a competitor and reduce the number of MNOs with nationwide networks in the United States from four to three. The combined company would have a retail market share larger than the two largest MNOs today, Verizon and AT&T. In some areas, including in the New York City metropolitan area, the combined company's share of subscribers would exceed 50%. The combined market share of Sprint and T-Mobile would result in an increase in market concentration that significantly exceeds the thresholds at which mergers are presumed to violate the antitrust laws. This increased market concentration will result in diminished competition, higher prices, and reduced quality and innovation.

They further claimed

> The cumulative effect of this merger, therefore, will be to decrease competition in the retail mobile wireless telecommunications services market and increase prices that consumers pay for mobile wireless telecommunications services. Preliminary estimates based on the submissions made by economists for Sprint and T-Mobile show that the merger could cost Sprint and T-Mobile subscribers at least $4.5 billion annually and the harm to all retail mobile wireless telecommunications subscribers could be even larger. The merger will also negatively impact the entire ecosystem of businesses and significant segments of the American economy that depend on mobile wireless telecommunications services.

The attorneys general are asking that T-Mobile and Sprint "be permanently enjoined from and restrained from carrying out the Merger."

GAO Reports on IT Workforce

The Government Accountability Office (GAO) released a report requested by a handful of House Members on information technology workforce planning activities. Like many other facets of IT and cybersecurity issues, the GAO found mixed progress that fell short of the intentions and goals laid out in statute and regulatory guidance. The GAO stated that it was asked to "conduct a government-wide review of federal IT workforce planning efforts…to examine the extent to which federal agencies have effectively implemented IT workforce planning practices." House Oversight and Reform Committee Ranking Member Jim Jordan (R-OH), Government Operations Subcommittee Chair Gerry Connolly (D-VA) and Ranking Member Mark Meadows (R-NC), and Representatives Will Hurd (R-TX) and Robin Kelly (D-IL) requested the report, and it is very possible they are looking at a hearing and/or legislation to address IT workforce issues.

The GAO offered agency specific recommendations, but time will tell if agencies will heed the GAO's advice and to what extent these recommendations will be implemented. The GAO noted its numerous reports on IT workforce planning, and the addition of "Improving the Management of Information Technology Acquisitions and Operations" to its High-Risk List in 2015. The agency also referenced its November 2016 IT workforce planning framework "that identifies four workforce planning steps and eight activities, including assessing gaps in competencies and skills, and developing strategies and plans to address those gaps…based on relevant laws and guidance issued over approximately the past 20 years."

Nonetheless, the GAO found

> Federal agencies varied widely in their efforts to implement key information technology (IT) workforce planning activities that are critical to ensuring that agencies have the staff they need to support their missions. Specifically, at least 23 of the 24 agencies GAO reviewed partially implemented, substantially implemented, or fully implemented three activities, including *assessing gaps in competencies and staffing*. However, most agencies minimally implemented or did not implement five other workforce planning activities…

The GAO concluded that "[a]gencies' limited implementation of the IT workforce planning activities has been due, in part, to not making IT workforce planning a priority, despite the laws and guidance which have called for them to do so for over 20 years." The agency cautioned that "[u]ntil this occurs, agencies will likely not have the staff with the necessary knowledge, skills, and abilities to

support the agency's mission and goals," and left implied by this conclusion is that IT procurement and management will also continue to suffer.

Trump Administration Commits To Fighting Election Interference

On November 5, Attorney General William Barr, Secretary of Defense Mark Esper, Acting Secretary of Homeland Security Kevin McAleenan, Acting Director of National Intelligence Joseph Maguire, FBI Director Christopher Wray, U.S. Cyber Command Commander and NSA Director Gen. Paul Nakasone, and CISA Director Christopher Krebs released a joint statement on their commitment to ensuring the security of next year's election:

> Election security is a top priority for the United States Government. Building on our successful, whole-of-government approach to securing the 2018 elections, we have increased the level of support to state and local election officials in their efforts to protect elections. The federal government is prioritizing the sharing of threat intelligence and providing support and services that improve the security of election infrastructure across the nation.
>
> In an unprecedented level of coordination, the U.S. government is working with all 50 states and U.S. territories, local officials, and private sector partners to identify threats, broadly share information, and protect the democratic process. We remain firm in our commitment to quickly share timely and actionable information, provide support and services, and to defend against any threats to our democracy.

These efforts come as Congress is divided on how it can best address election security with Democrats favoring legislation and funding to revamp the security of state voting systems with many Republicans balking while others prefer appropriating more funding for the Election Assistance Commission. Recent Democratic attempts to bring a range of election security bills to the Senate floor were blocked by Republicans, and House-passed legislation has similarly not been considered in the Senate. However, the Appropriations Committees have included funding for grants to states for election security in their respective FY 2020 Financial Services and General Government Appropriations Acts (H.R. 3351/S. 2524) of $600 million in the House bill and $250 million in the Senate bill. The FY 2018 Consolidated Appropriations Act (P.L. 115-141) included $380 million for this program.

Further Reading

- "The Porch Pirate of Potrero Hill Can't Believe It Came to This" – *The Atlantic*. How technology intersects with and possibly exacerbates long entrenched societal problems. A fascinating read starting with someone stealing Amazon packages in a rapidly gentrifying San Francisco neighborhood.
- "Why Do We Tolerate Saudi Money in Tech?" – *The New York Times* and "Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics" – *The Washington Post*. Unsealed indictments show that agents working for the Saudi regime used Twitter to track critics of the government, and questions have been posed regarding the effect of a Saudi prince's stake in Twitter that is the second largest bloc of shares and bigger than CEO Jack Dorsey. It is likely that many countries around the world will continue to seek to penetrate Twitter and other giant social media platforms to mine the information for a range of goals, not least of which will be spying on enemies.

- "Facebook's Rebrand Addresses Its $5 Billion FTC Settlement" – *BuzzFeed News*. Critics claim Facebook's all capitals rebrand is an attempt to forestall action by regulators that its ownership of WhatsApp and Instagram is deceptive and to also to stave off attempts to split up the company.
- "Inside the Valentine's Day Text Message Mystery" – *The New York Times*. Last week thousands of SMS messages sent on Valentine's Day 2019 arrived on people's phones, causing understandable confusion. The explanations from telecommunications companies as to why this happened were vague, but eventually the fingered was pointed at Syniverse Technologies, a third-party messaging service that admitted the wave of messages was caused when a server that crashed on February 14 was reactivated.
- "In the Trump era, Oracle holds tech sway" – *Axios*. In part because of CEO Safra Catz's support for President Donald Trump, and in part because of its different business model, Oracle has escaped the lashing the larger technology companies have endured of late.
- "Facebook considering limits on targeted campaign ads" – *Politico*. Vice-President for Global Affairs and Communications and former British Deputy Prime Minister Nick Clegg reveals that Facebook may forgo the microtargeting of users that allowed for personalized political ads in 2016 that many argue amplified the dynamics of the 2016 election and allowed disinformation to be all the more effective. Facebook's floating of this policy change came after Google signaled it might limit political advertising, and Twitter swore off paid political ads. These may be signs that the scrutiny and pressure that accompany political advertising may not be worth the revenue.
- "Why has a privacy app used by Edward Snowden hit the NBA, NFL and NCAA?" – *yahoo! sports*. Signal has displaced WhatsApp as the go-to messaging in professional North American sports for players, agents, and executives because of the app's reputation as the safest, most secure app available. It also helps cover potentially unethical conduct because of the setting that automatically deletes communications.