Michael Kans' Technology Policy Update
8 May 2019
By Michael Kans, Esq.

Senate Privacy Hearing

On May 1, the Senate Commerce, Science, and Transportation Committee held a hearing entitled "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework."

The witnesses appearing before the committee were:

- Ireland's Data Protection Commissioner Helen Dixon
- American Civil Liberties Union Senior Legislative Counsel Neema Singh Guliani
- Future of Privacy Forum Chief Executive Officer Jules Polonetsky
- Common Sense Media Chief Executive Officer and Founder Jim Steyer

Chairman Roger Wicker (R-MS) asserted that "[t]he consumer benefits of a data-driven economy are undeniable…[and] [t]hese benefits are what fuel the vibrancy and dynamism of today's Internet marketplace." He stated that "[d]espite these benefits, however, near-daily reports of data breaches and data misuse underscore how privacy risks within the data-driven economy can no longer be ignored." Wicker said that "[t]he increased prevalence of privacy violations threatens to undermine consumers' trust in the Internet marketplace…[and] [t]his could reduce consumer engagement and jeopardize the long-term sustainability and prosperity of the digital economy."

Wicker stated that "[t]o maintain trust, a strong, uniform federal data privacy framework should adequately protect consumer data from misuse and other unwanted data collection and processing…[and] [w]hen engaging in commerce, consumers should rightly expect that their data will be protected." He said that "I hope witnesses will address how a federal privacy law should provide consumers with more transparency, choice, and control over their information to prevent harmful data practices that reduce consumer confidence and stifle economic engagement." Wicker said that "[t]o provide consumers with more choice and control over their information, both the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) provide consumers with certain privacy rights." He added that "[s]ome of these rights include the right to be informed or the right to know; the right of access; the right to erasure or deletion; the right to data portability, and the right to non-discrimination, among others." He stated that he hopes the "witnesses will address how to provide these types of rights within a United States federal framework without unintentionally requiring companies to collect and retain more consumer data. Provisioning certain privacy rights to individuals, without minimum controls, may have the opposite effect of increasing privacy risks for consumers."

Wicker said that "[i]n developing a federal privacy law, the existing "notice and choice" paradigm also has come under scrutiny…[and] [u]nder notice and choice, businesses provide consumers with notice – typically through a lengthy and worthy privacy policy – about their data collection and processing practices." He said that "[c]onsumers are then expected to make a "take it or leave it" choice about whether or not to purchase or use a product or service, but is this really a choice?" Wicker said that "I hope witnesses will address how to ensure that consumers have access to simplified notices that offer meaningful choices about what information an organization collects about them, instead of lengthy and confusing privacy notices or "terms of use" that are often written

in legalese and bury an organization's data collection activities." He added that "I also hope witnesses will speak to ways in which Congress can provide additional tools and resources for consumers to make informed privacy decisions about the products and services they choose to use both online and offline." Wicker asserted that "[f]undamental to providing truly meaningful privacy protections for consumers is a strong and consistent federal law…[and] [t]his is critical to reducing consumer confusion about their privacy rights and ensuring that consumers can maintain the same privacy expectations across the country."

Ranking Member Maria Cantwell (D-WA) remarked I the two months since the last full committee hearing on privacy, "consumer data has continued to be mishandled." She said "it's clear that companies have not learned from past failures, and at the expense of consumers, we are seeing that self-regulation is insufficient." Cantwell stated that "just days ago, cybersecurity researchers revealed the existence of a massive cloud data breach left wide open and unprotected, containing full names, addresses, dates of birth, income, and marital status on more than 80 million U.S. households." Cantwell said this blatant disregard of safety and security makes clear why the heating is necessary. She said that Microsoft recently revealed an unknown number of web email accounts were compromised, and that there have been further Facebook privacy lapses. Cantwell asked how Congress can create a culture of data security that protects consumers and allows commerce to continue to grow.

Cantwell said consumers continue to be bombarded by threats to their privacy and cybersecurity adversaries get more organized day-by-day. She said it is crucial that policymakers understand privacy on a data security spectrum. Cantwell called for a more proactive approach to cybersecurity that does more to protect consumers, which becomes especially important in the age of Internet of Things (IoT). She remarked on a subcommittee hearing held the day before, which contemplated the prospect of billions of devices collecting data all the time, leading to billions of entry points. Cantwell said that the internet is global and therefore threats can come from anywhere. She said this is why it is important to have a national strategy and to work with international partners to craft cyber norms and work towards harmonizing privacy and cybersecurity regulations.

Cantwell said consumers are at the center of the issue, and the solution cannot be that they have a better sense of the risks involved. She said Congress needs to make sure that their concerns are not met with notice and consent. Cantwell remarked that the best plain language notices, the clearest opt-in consent provisions, and the most crystal clear transparency does not do any good when companies are being careless and allowing third parties to access the data that have no relationship to the consumer. She said that the culture of monetizing consumer data at every twist and turn needs to be coupled to data security. Cantwell said she knows Wicker is committed to comprehensive legislation and said any such bill should address security and privacy for the entire lifecycle of data collection to storage and to processing.

Guliani stated detailed the ACLU's position on the necessary features of federal privacy legislation:

- Any federal privacy standards should be a floor — not a ceiling — for consumer protections. The ACLU strongly opposes legislation that would, as some industry groups have urged, preempt stronger state laws. Such an approach would put existing consumer protections, many of which are state-led, on the chopping block and prevent additional consumer privacy protections from ever seeing the light of day. We also oppose efforts to limit the ability of state Attorneys General or other regulators from suing, fining, or taking other actions against companies that violate their laws.

- Federal privacy legislation will mean little without robust enforcement. Thus, any legislation should grant greater resources and enforcement capabilities to the FTC and permit state and local authorities to fully enforce federal law. To fill the inevitable government enforcement gaps, however, the ACLU urges Congress to ensure that federal legislation also grants consumers the right to sue companies for privacy violations.
- Existing federal laws prohibit discrimination in the credit, employment, and housing context. Any federal privacy legislation should ensure such prohibitions apply fully in the digital ecosystem and are robustly enforced. In addition, we urge Congress to strengthen existing laws to guard against unfair discrimination, including in cases where it may stem from algorithmic bias.
- Legislation must include real protections that consider the modern reality of how people's personal information is collected, retained, and used. The law should limit the purposes for which consumer data can be used, require purging of data after permissible uses have completed, prevent coercive conditioning of services on waiving privacy rights, and limit so-called "pay for privacy" schemes. Otherwise, we risk ending up in the same place we began — with consumers simply checking boxes to consent with no real understanding of or control over how their data will be used.

Polonetsky said that "Congress should advance a baseline, comprehensive federal privacy law because the impact of data-intensive technologies on individuals and vulnerable communities is increasing every day as the pace of innovation accelerates."

Polonetsky offered the following suggestions:

- In drafting baseline federal privacy legislation, the most important decision is one of scope: how should the law define the "personal information" that is to be protected? Laws that adopt an overly broad standard are forced to include numerous exceptions in order to accommodate necessary or routine business activities, such as fraud detection, security, or compliance with legal obligations; or to anticipate future uses of data, such as scientific research or machine learning. Conversely, laws that define personal information too narrowly risk creating gaps that allow risky uses of data to go unregulated.
- The term sensitive data is used to refer to certain categories of personal data that require additional protections due to the greater risks for harm posed by processing or disclosing this data. While individuals should generally be able to exercise reasonable control over their personal information, those controls should be stronger with respect to sensitive data. Thus, a federal privacy law should provide heightened protections for the collection, use, storage, and disclosure of users' sensitive personal information or personal information used in sensitive contexts.
- It is vital that a national privacy law be crafted in a way that does not unduly restrict socially beneficial research, and that policymakers at the local, state, and federal levels continue to have the information they need to make evidence-based decisions. Today, in addition to the entities governed by the HIPAA Rule and legal mandates around human subject research, many private companies also conduct research, or work in partnerships with academic researchers, to gain important insights from the data they hold.
- A federal baseline privacy law should incentivize companies to employ meaningful internal accountability mechanisms, including privacy and security programs, which are managed by a privacy workforce. Ultimately, to implement privacy principles on the ground, including not just legal compliance but also privacy by design and privacy engineering, organizations will need to devote qualified and adequately trained employees. Indeed, over the past

two decades, a privacy workforce has developed that combines the fields of law, public policy, technology, and business management.

- Federal privacy legislation should promote the use of technical solutions, including privacy-enhancing technologies (PETS). The "holy grail" for data protection is utilizing technology that can achieve strong and provable privacy guarantees while still supporting beneficial uses. Legislation should create specific incentives for the use of existing privacy-enhancing technologies and for the development of new PETS.

Senate IoT Hearing

The Senate Commerce, Science, and Transportation Committee's Security Subcommittee held a hearing titled "Strengthening the Cybersecurity of the Internet of Things." The subcommittee heard from the following witnesses:

- Consumer Technology Association Technology & Standards Vice President Michael Bergman
- Mr. Matthew Eggers, Vice President, Cybersecurity Policy, U.S Chamber of Commerce
- Mr. Harley Geiger, Director of Public Policy, Rapid7
- Mr. Robert Mayer, Senior Vice President for Cybersecurity, US Telecom – The Broadband Association
- Dr. Charles Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology

Chair Dan Sullivan (R-AK) said in the increasingly interconnected world, the Internet of Things (IoT) delivers substantial benefits to end users. He said that by 2020, the number of connected devices may exceed 50 billion, offering a wide range of new capabilities for consumer products. Sullivan remarked that the new technologies are subject to "unprecedented security challenges" that are becoming increasingly apparent with each passing day. He said that cyber-crime and cyber-espionage has serious impacts on consumers and companies, including damage to company performance, trade, competitiveness, and innovation for the U.S. writ large. Sullivan said that estimates of the annual global cost of cyber-crime range from $375-575 billion. He claimed that China is a major player in cyber-espionage and these activities continue against U.S. companies despite high-level Chinese government assurances that these activities would be discontinued. Sullivan stated that these state-driven cyber-attacks give state-sponsored enterprises an edge in international deals, specifically through access to bid prices, contracts, and mergers and acquisitions let alone the damage this does to U.S. national security. He said it has been estimated that China was the number one source for IoT attacks in 2018. Sullivan declared that sound security practices must keep pace with the IoT in order to mitigate threats. He said that over the last few years the committee has supported the public-private partnership approach to cybersecurity, including the enactment of the "Cybersecurity Enhancement Act" to provide for the development of a voluntary framework to reduce cyber risks to critical infrastructure as well as Senate passage of the DIGIT Act (S. 88 (115)) to establish a working group to encourage the growth of IoT. He said the hearing would focus on furthering public-private partnerships, including through efforts to better secure the cyber universe through standards that are voluntary, flexible, performance-based, and cost-effective.

Ranking Member Ed Markey (D-MA) noted that he convened two hearings on cybersecurity in 1993 when he chaired the Telecommunications Subcommittee in the House. He said that those hearings were conducted in the before-Facebook era, and the present moment is far more dangerous. Markey said that even then it was clear that developing a national policy on cybersecurity was

important for U.S. security and competitiveness. He said that now is the time for such a policy, and as the committee is working on developing privacy legislation, it is vital that a robust cybersecurity regime also be included that truly protects the American public, industries, and government institutions from the "sinister side of cyberspace." Markey said Americans should have a Privacy Bill of Rights, including the right to tell companies they cannot share or sell their personal information without consent. He added that it is not possible to secure one's privacy without ensuring that one's personal information is protected from hackers. Markey said that while IoT holds vast promise to improve the lives of Americans, it also poses immense threats. He said that cyber vulnerabilities will continue to pose a direct threat to economic prosperity, privacy, and U.S. security. Markey noted the bill he introduced, the "Cyber Shield Act," (S. 2020 (115)), which would create a voluntary certification program for IoT.

Geiger stated that "Rapid7 has four recommendations for Congress:

1) Require reasonable security of personal information. Security of personal information is fundamental to privacy and should be included in any privacy legislation. Legislation that requires risk-based security requirements for personal information will apply to IoT devices collecting and processing that information. This will strengthen some aspects of IoT security in sectors that are otherwise not covered by the jurisdiction of federal agencies.

2) Support coordinated but enforceable agency actions on IoT security based on industry standards. Federal agencies should be empowered to require reasonable security for IoT, including security-by-design principles, within their areas of jurisdiction. To the extent possible, agency requirements should be harmonized by following a consistent baseline supported by industry standards. Voluntary guidance should not replace formal accountability and enforcement mechanisms when baseline security is not met. Congress should exercise its oversight role to ensure agency efforts are effective in strengthening IoT security.

3) Facilitate voluntary transparency programs for consumer IoT security. Congress should support voluntary consumer awareness programs to enhance the transparency of critical security features of consumer IoT devices, such as certifications, seals, or labels. Providing consumers with clear information about critical security features in IoT devices will foster market competition based on security, promote innovation insecurity, and build trust in the security of IoT products.

4) Avoid new regulations that chill beneficial security research. Any new regulations related to IoT should not undermine cybersecurity by imposing blanket access and use restrictions that hinder independent research and repair. Independent security researchers, acting in good faith, that identify and disclose vulnerabilities in coordination with IoT manufacturers can advance security by boosting the likelihood of remediating otherwise unaddressed vulnerabilities.

Romine highlighted several National Institute for Standards and Technology (NIST) initiatives:

- Considerations for Managing IoT Cybersecurity and Privacy Risks: NIST Internal Report 8228 (NISTIR 8228)In recognition of a critical cybersecurity gap, NIST released draft NIST Internal Report 82283, Considerations for Managing IoT Cybersecurity and Privacy Risks in September 2018. The purpose of this publication is to help organizations better understand and manage the cybersecurity and privacy risks associated with IoT devices throughout their lifecycles. This publication emphasizes what makes managing these risks different for IoT devices than conventional IT devices, and it omits all aspects of risk management that are largely the same for IoT and conventional IT. The publication provides insights to inform organizations' risk management processes. For some IoT devices, additional types of risks,

including safety, reliability, and resiliency, need to be managed simultaneously with cybersecurity and privacy risks because of the effects addressing one type of risk can have on others. Only cybersecurity and privacy risks are in scope for this publication.

- Status of International Cybersecurity Standardization for IoT: NIST Internal Report 8200 (NISTIR 8200)NIST Interagency Report 82004, published in November 2018, examines the current state of international cybersecurity standards development by voluntary consensus standards bodies for IoT. NISTIR 8200 is intended for use by the government and the broader public. The report aims to inform and enable policymakers, managers, and standards participants as they seek timely development and use of such standards in IoT components, systems, and related services.
- Considerations for a Core IoT Cybersecurity Capabilities Baseline. On February 4, 2019, NIST published a discussion draft7 to gather feedback to help identify core IoT cybersecurity capabilities that are most vital for IoT devices. Through NIST research, related stakeholder engagement, comments received during the NISTIR 8228 public comment period, and, as described above, in the Botnet Report, NIST identified a critical gap area in guidance on baselines for IoT device cybersecurity. In particular, there was interest in baselines focused on the pre-market cybersecurity capabilities that could be built into the products, as opposed to the cybersecurity controls that consumers or organizations that use IoT in their enterprise operations, could apply post-market.

Eggers summarized the Chamber of Commerce's views:

- Industry and National Institute of Standards and Technology (NIST) leadership. The business community, NIST, and other stakeholders are developing a core cybersecurity capabilities baseline for Internet of Things (IoT) devices. A top U.S. Chamber of Commerce priority for industry is to achieve consensus on the technical criteria that support the IoT cyber baseline.
- A win-win cybersecurity market. The Chamber wants device makers, service providers, and buyers to gain from the development of state-of-the-art IoT components and sound risk management practices.
- Global, industry-driven standards and practices. The Chamber believes that IoT cyber efforts will be most effective if they reflect global standards and industry-driven practices. A fragmented global cybersecurity environment creates uncertainty for industry and splinters the resources that businesses devote to device development, production, and assessments.

CCPA Fixes Advance

There has been continued action on amending the "California Consumer Privacy Act" (A.B. 375) (CCPA) with eight bills being approved by the primary committee of jurisdiction in the California Assembly, and a bill to expand a consumer's private right of action having possibly stalled in the California Senate. As expected, the California legislature is considering fixes and amendments to the hastily drafted and passed statute even after a package of fixes was enacted last year. The statute remains problematic and some of these bills would address some of these issues.

The Consumer and Privacy Protection Committee released the following summaries of the approved bills:

- **A.B. 25:** This bill would clarify the definition of consumer under the CCPA to exempt a person's personal information (PI) only to the extent that their PI is collected and used solely within their employee role, or in similar roles within the employment context, as specified. This bill would also reflect the Legislature's intent to ensure that a business complies with a

consumer's request for specific pieces of information in a privacy protective manner, as specified.

- **A.B. 846:** This bill would replace the "financial incentive programs" provisions in the nondiscrimination statute of the CCPA with an authorization for offerings that include, among other things, gift cards or certificates, discounts, payments to consumers, or other benefits associated with a loyalty or rewards program, as specified.
- **A.B. 873:** This bill would narrow the definition of personal information (PI) in the CCPA to: (1) exclude information that "is capable of being associated with" a particular consumer; (2) exclude information that could be linked to particular "households"; and, (3) potentially exclude items that are otherwise listed as types of PI even if those items actually identify a particular consumer. This bill would also revise a provision of the CCPA prohibiting the act from being construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered PI. Lastly, this bill would replace the CCPA's current definition of "deidentified."
- **A.B. 874:** This bill would expand the "publicly available" information that is exempted from the definition of "personal information" (PI) in the CCPA to ensure that "publicly available" information includes any information that is lawfully made available from government records. This bill would also correct a drafting error in the definition of "PI" to clarify that PI does not include deidentified or aggregate consumer information.
- **A.B. 981:** This bill would exempt insurance institutions, agents, and support organizations (insurers) to which the Insurance Information and Privacy Protection Act (IIPPA) applies from the CCPA, except as specified. The bill would also, among other things, incorporate specific concepts from the CCPA into the IIPPA.
- **A.B. 1146:** This bill would establish an additional exemption from the CCPA for vehicle and ownership information shared pursuant to or in anticipation of a vehicle repair relating to warranty work or a recall conducted pursuant to federal law, except with respect to a consumer's right to access their personal information (PI), to know what PI has been collected or sold about them, and to bring a private right of action in the case of a data breach.
- **A.B. 1355:** This bill would address various drafting errors and make other clarifying changes in the California Consumer Privacy Act of 2018 (CCPA). Specifically, this bill would: 1) Correct a drafting error in the CCPA's definitions to specify that "personal information" (as opposed to "publicly available") does not include consumer information that has been deidentified or aggregate consumer information. 2) Address duplicative language in the CCPA relating to a consumer's right to know what personal information (PI) has been collected about them. 3) Clarify that consumers who are at least 13 years of age and less than 16 years of age (as opposed to "between 13 and 16 years of age") have the right to opt-in to the sale of their PI. 4) Align various requirements throughout the CCPA, such as with respect to the information that must be disclosed about the categories of third parties to which a business has sold PI, as specified. 5) Correct various cross-references and include missing cross-references to appropriate CCPA provisions. 6) Correct various drafting errors and make other clarifying or technical, non-substantive changes.
- **A.B. 1564:** This bill would revise a requirement in the CCPA for businesses to make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA, including, at a minimum, a toll-free telephone number and, if the business maintains an internet website, a website address. Instead, this bill would require that businesses: (1) make available to consumers either a toll-free telephone number or an email address; and, (2) if the business maintains an internet website, make an internet website available to consumers to submit requests for information

required to be disclosed pursuant to specified provisions of the CCPA. This bill would make other technical, non-substantive changes.

Some of these bills may subsequently be considered by other committees of jurisdiction, and it is not clear when the Assembly may consider these bills.

However, the committee opted against considering a bill supported by privacy and civil liberties advocates, the "Privacy for All Act" (A.B. 1760), that would have expended the scope of the CCPA. Again, the committee provided a summary:

- **A.B. 1760:** This bill seeks to re-establish the consumer rights and business obligations of the CCPA to be based on the "sharing" of a consumer's personal information (PI) by a business, instead of the "sale" of a consumer's PI (which includes sharing if for valuable consideration). This bill would generally modify the rights and obligations of the CCPA to: (1) change the law from an "opt-out" and "opt-in" hybrid dependent on the age of the consumer, to, instead, provide a right for consumers of any age to "opt-in" before a business may share their PI; (2) remove any ability for businesses to provide certain financial incentives that are nondiscriminatory, as specified under the CCPA; (3) limit the use and retention of PI by a business to what is reasonably necessary to provide a service or conduct an activity, as specified, subject to certain exceptions; (4) broaden the duties of businesses in connection with CCPA sections governing the disclosure, access, and deletion of consumer information, while also narrowing certain CCPA exemptions (including exemptions specific to the right of deletion); (5) repeal any right to cure for businesses; (6) repeal the authorization for businesses to seek guidance related to compliance from the Attorney General's (AG) office; and (7) redefine various terms. This bill would also revise the CCPA's public enforcement provision to additionally authorize a county district attorney, a city attorney, or a county counsel to bring a civil action, in the name of the of the people of the State of California, against any business, service provider, or other person that violates the CCPA. This bill would delay the operative date of the CCPA by an additional year, to January 1, 2021 and make other conforming or technical changes.

In a related development, the Senate Appropriations Committee opted against considering a bill (S.B. 561) developed by California Attorney General Xavier Becerra and Senate Judiciary Committee Chair Hannah-Beth Jackson. The committee put the bill in its suspense file, which is reputedly where legislation often dies. SB 561 would eliminate the requirement that the California Department of Justice must furnish an opinion to a business or other entity with "guidance on how to comply with the provisions" of the CCPA. The legislation would also expand the private right of action available to California residents. Now, they may sue if their rights are violated as opposed to the current statutory language limiting actions to "consumers whose nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Finally, the bill would remove the current 30-day window in which businesses alerted to CCPA violations can "cure" the noncompliance. Moreover, SB 561 would allow the Attorney General to sue for an injunction and civil penalties of $2,500 per violation or $7,500 per "intentional violation."

NIST Privacy Framework Discussion Draft Released

The National Institute of Standards and Technology (NIST) has released a Privacy Framework Discussion Draft for comment. As the ultimate fate of federal privacy legislation is not currently clear, NIST's Privacy Framework may prove to be a national guideline much like the Cybersecurity Framework has. NIST is asking for "Feedback" on this discussion draft that "may be sent to privacyframework@nist.gov, but will not be posted online." Additionally, NIST will be holding "NIST Privacy Framework: Workshop #2 on May 13-14, 2019, at the Georgia Tech Scheller College of Business in Atlanta, Georgia" to further develop the Privacy Framework.

In November 2018, NIST released a request for information (RFI) "to help identify, understand, refine, and guide development" of the "NIST Privacy Framework: An Enterprise Risk Management Tool." At that time, NIST articulated its intention that the Privacy Framework will be "for voluntary use" and "is envisioned to consist of outcomes and approaches that align policy, business, technological, and legal approaches to improve organizations' management of processes for incorporating privacy protections into products and services."

In terms of the conceptual backdrop, NIST explained that "[c]ybersecurity risks arise from unauthorized activity related to the loss of confidentiality, integrity, or availability of a system or information asset…[but] privacy risks arise as a byproduct of intentional (i.e., authorized) data processing occurring in systems, products, and services that help organizations lead to unintended problems or to achieve their mission/business objectives." NIST asserted that "privacy risk can be understood as the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur."

NIST explained that "[t]he Privacy Framework has been developed to improve privacy risk management for organizations delivering or using data processing systems, products, or services in any sector of the economy or society, regardless of their focus or size." NIST stated that "[t]o enable innovation and increase trust in systems, products and services, NIST has developed the voluntary [Privacy Framework] to help organizations consider:

- How their systems, products, and services affect individuals; and
- How to integrate privacy practices into their organizational processes that result in effective solutions to mitigate these impacts and protect individuals' privacy."

Like the Cybersecurity Framework, the Privacy Framework "is composed of three parts: the Core, the Profiles, and the Implementation Tiers:

- The Core is a set of privacy protection activities and desired outcomes that allows for communicating prioritized privacy protection activities and outcomes across the organization from the executive level to the implementation/operations level. The Core consists of five concurrent and continuous functions—Identify, Protect, Control, Inform, and Respond. Together these functions provide a high-level, strategic view of the life cycle of an organization's management of privacy risk. The Core then identifies underlying key categories and subcategories—which are discrete outcomes—for each function.
- A Profile represents the privacy outcomes the organization aims to achieve. To develop a Profile, an organization can review all of the functions, categories, and subcategories to determine which are most important to achieving the desired privacy outcomes, based on business/mission drivers, types of data processing, and individuals' privacy needs. The organization can create or add functions, categories, and subcategories as needed. Profiles can be used to identify opportunities for improving privacy posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). Profiles can

be used to conduct self- assessments and to communicate within an organization or between organizations about how privacy risks are being managed.

- Implementation Tiers ("Tiers") provide context on how an organization views privacy risk and whether it has adequate processes and resources in place to manage that risk. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. When selecting Tiers, an organization should consider its current risk management practices; its data processing systems, products, or services; legal and regulatory requirements; business/mission objectives; organizational privacy values and individuals' privacy needs; and organizational constraints.

NIST included this diagram to map the Cybersecurity Framework's Core functions against their proposed Core functions for the Privacy Framework:

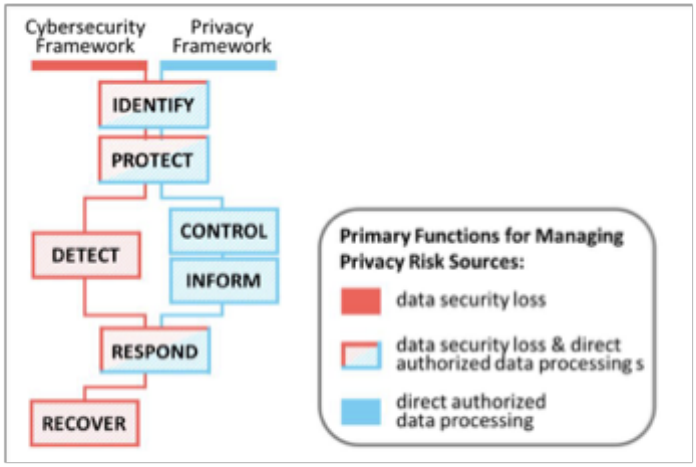

Figure 2: Cybersecurity Framework and Privacy Framework Functions Relationship

Of course, this is one part of the Trump Administration's approach on how it will address privacy concerns. In September 2018, the National Telecommunications and Information Administration (NTIA) issued a request for comments (RFC) "on a proposed approach to consumer data privacy designed to provide high levels of protection for individuals, while giving organizations legal clarity and the flexibility to innovate." At that point, NTIA noted that

> This RFC is the outcome of an interagency process led by the National Economic Council (NEC) of the United States. NTIA has worked in coordination with the International Trade Administration (ITA) to ensure consistency with international policy objectives, and in parallel with the work of the National Institute of Standards and Technology (NIST) in developing a voluntary risk-based Privacy Framework as an enterprise risk management tool for organizations. In developing this RFC, the Department conducted significant outreach to a diverse set of individuals and organizations, including a broad range of industries, academics, and civil society organizations. These meetings helped to shape this Administration's proposed general approach to privacy...

NTIA stated that "[t]his approach is divided into two parts:

> (1) A set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and

(2) a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections.

CISA Names National Critical Functions

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has announced a new initiative, "National Critical Functions," that will reorient the federal government's view on risks to U.S. critical infrastructure holistically instead of the approach relying on a sector-specific regime, including cyberecurity. Not surprisingly, these National Critical Functions sweep across the U.S. economy from telecommunications to banking to financial services to transportation and other areas. Ultimately, CISA will create a Risk Register, a process by which the agency could gameplan to "prioritiz[e] areas of national risk to critical infrastructure in need of mitigation and collective action." CISA released a summary, a high-level memorandum, and the National Critical Functions themselves (also cut and pasted below), but beyond these sparse documents, at this point, it is hard to foresee the practical implications of the new initiative.

CISA asserted that "[t]he National Critical Functions construct provides a risk management approach that focuses on better understanding the functions that an entity enables or to which it contributes, rather than focusing on a static sector-specific or asset world view." CISA asserted that "[t]his more holistic approach is better at capturing cross-cutting risks and associated dependencies that may have cascading impact within and across sectors. It also allows for a new way to view criticality, which is linked to the specific parts of an entity that contribute to critical functions...[and] [b]y viewing risk through a functional lens, we can ultimately add resilience and harden systems across the critical infrastructure ecosystem in a more targeted, prioritized, and strategic manner."

CISA uses a definition of "National Critical Functions" as "[t]he functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof," which as best as I can tell was first used in a recent executive order on electromagentic pulses (EMP) and it similar to a definition coined in the USA PATRIOT Act of "critical infrastructure:" "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." It appears as if the new definition sets the bar lower for the type of harm the federal government is looking to fend off. It is quite likely this definition migrates to Office of Management and Budget (OMB) memoranda and other agency guidance begin to use the new, expanded definition.

CISA claimed that "[t]he National Critical Functions are a springboard for a wide range of risk management activity including:

- Supporting Infrastructure and Programmatic Prioritization
- Conducting Detailed Operational and Risk Analysis
- Informing Intelligence Collection Requirements
- Supporting Incident Management Prioritization
- Setting Priorities for Investments in Infrastructure Security and Resilience
- Supporting National Security Decision Making
- Enhancing the Efficacy of Continuity Efforts

As mentioned earlier, the new "National Critical Functions construct" will entail "the development of a Risk Register." CISA explained that "[b]y performing risk and dependency analysis and consequence modeling, CISA will identify scenarios that could potentially cause national-level degradation to National Critical Functions." CISA stated that "[t]his will result in a tiered Risk Register – prioritizing areas of national risk to critical infrastructure in need of mitigation and collective action." CISA added that "[t]he process for developing the Risk Register will involve representatives from across government and industry and combine analysis, with policy judgment and operational insight." In developing this Risk Register, "CISA will be looking for information to help answer the question of "what keeps you up at night:"

- Scenarios: identifying scenarios that could plausibly cause National-level degradation of NCFs.
- Risk Attributes: identifying likelihood and consequence information associated with each scenario leveraging existing sources, such as sector risk assessments, where possible.
- Dependencies: mapping out how disruptions to one NCF could cascade and impact other NCFs.
- Readiness: gauging existing risk management efforts and the degree that stakeholders are ready to further engage in communitywide efforts to mitigate risks.

Finally, "[t]he Risk Register will be a document developed by CISA that we also intend to share as appropriate within the critical infrastructure community – including Government and Sector Coordinating Councils...[but] [p]ortions of the Risk Register may have higher classification levels."

National Critical Functions

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access and Connection Services ▪ Provide Positioning,	▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and	▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government	▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food

National Critical Functions

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services	Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit	▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services	Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

National Critical Functions

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
		▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health	

President Signs Cyber Workforce EO

The President has signed an executive order (EO) on the U.S.'s cybersecurity workforce with one section aimed at improving the federal government's cyber workforce and another for the balance of the American cyber workforce. This EO flows from EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," and a report it required, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future."

There are a suite of interconnected directives regarding the federal government's cyber workforce. The heads of agencies are charged generally with "ensuring the effectiveness of their cybersecurity workforces." DHS must "establish a cybersecurity rotational assignment program, which will serve as a mechanism for knowledge transfer and a development program for cybersecurity practitioners" and must submit a plan to the President within 90 days on this program.

However, there is also legislation that would establish a rotational program. This week, the Senate passed the "Federal Rotational Cyber Workforce Program Act of 2019" (S. 406) by unanimous consent. The bill would "create a rotational cyber workforce program in which Federal employees in cyber workforce positions can be detailed to another agency to perform cyber functions…[and] will enable Federal cyber workforce employees to enhance their cyber skills with experience from executing the cyber missions of other agencies" according to the Committee Report. No companion

has been introduced in the House, however. It is possible that lawmakers will wait to see how the Administration's rotational program works out before passing a bill.

However, of possible greatest immediate impact to federal contractors, the General Services Administration (GSA), the Office of Management and Budget (OMB), and the Department of Commerce must incorporate the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) "lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services." These agencies must also "[e]nsure that contracts for information technology and cybersecurity services include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the NICE Framework." By May 2019, GSA, OMB, and the Department of Commerce must submit a report to the White House that "describes how the NICE Framework has been incorporated into contracts for information technology and cybersecurity services, evaluates the effectiveness of this approach in improving services provided to the United States Government, and makes recommendations to increase the effective use of the NICE Framework by United States Government contractors."

The EO details the actions aimed at bolstering the U.S.'s cyber workforce. The Departments of Commerce and Homeland Security must "develop a consultative process that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners to assess and make recommendations to address national cybersecurity workforce needs and to ensure greater mobility in the American cybersecurity workforce" with "priority consideration will be given to the following imperatives:

> (i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;
> (ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;
> (iii) To align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and
> (iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments."

Moreover, this report should rely on the recommendations in the aforementioned "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future."

Within six months, the Departments of Defense, Transportation, Energy, and Homeland Security must submit a report that

> (i) Identifies and evaluates skills gaps in Federal and non-Federal cybersecurity personnel and training gaps for specific critical infrastructure sectors, defense critical infrastructure, and the Department of Defense's platform information technologies; and
> (ii) Recommends curricula for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

The Departments of Commerce, Labor, Education, and Homeland Security must "encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non profit, and private-sector entities, consistent with applicable law."

OMB Seeks To Revamp Shared Services

The Office of Budget and Management (OMB) has released a memorandum that proposes to change how the federal government will buy certain core services that almost all agencies use (e.g. human resources). This revamp of the Shared Services initiative is a part of the President's Management Agenda (PMA) and is closely related in spirit to the Category Management initiative the Trump Administration also reformed a few weeks ago. In relevant part, if implemented as planned, federal agencies may look to the Department of Homeland Security for buying cybersecurity services as opposed to each agency buying its own. All Chief Financial Officers Act agencies would be subject to this memorandum, meaning independent agencies are excluded (e.g. the Securities and Exchange Commission or the Federal Trade Commission), but the Department of Defense is included.

Of course, there is a process under which an agency could make the case that the shared service they might normally expected to buy does not meet their particular needs. And, as with all government-wide initiatives, the key will be in follow through from OMB in enforcing the new regime and buy-in at the top of agencies and among key personnel in components, for, as we have seen, without these, these changes, like many other recent changes to acquisition practices, will likely affect marginal changes.

OMB explained that "[t]his memorandum is a strategy based on industry experiences, and lessons learned from other central governments that will reduce duplication, improve accountability, and improve Federal shared services." OMB claimed that "[t]his updated strategy will enable the delivery of an innovative, flexible, and competitive set of solutions and services."

OMB stated that "[t]his memorandum:

- Describes the process and desired outcomes for shared services;
- Establishes a process for designating agencies as Quality Services Management Offices (QSMOs);
- Establishes the governance and accountability model that will be used to engage customers and enable QSMO performance excellence, including the Shared Services Governance Board (SSGB) and the Business Standards Council (BSC);
- Requests that all CFO Act agencies appoint a Senior Accountable Point of Contact (SAPOC) to coordinate actions across the agency to support adoption of the shared service strategies; and
- Rescinds previous OMB memoranda that are no longer aligned to this strategy.

OMB stated that "[i]mmediate implementation of this strategy requires the Government to define and execute an integrated approach to shared services including:

1. Developing inter-agency standards and priorities for shared services;
2. Creating centralized capabilities, shared governance, and performance expectations; and
3. Continuing to expedite the adoption of existing quality services that currently perform well and provide demonstrated value to agency customers.

OMB stated that "[o]nce an opportunity for centralization or sharing is identified, OMB will designate a lead agency as the QSMO to take responsibility for establishing and/or managing such capabilities." OMB noted that "[t]he Government's current shared services model relies on a network of legacy providers (designated or self-selected) to deliver specific shared services...[and] [a]s QSMOs become operational, there may be technology or services that are beneficial for legacy providers to continue offering to agencies for a finite period." In this case, the agency would need to clear the use of legacy services with OMB. The memorandum also details a process under which an agency might "issue new solicitations for new or modernized technology or services" outside the new shared service (e.g. human resources IT), and the agency must make the business case approved by a number of stakeholders in the agency and OMB.

OMB stated that "[o]ne of the PMA's primary focus areas centers on the Sharing Quality Services Cross Agency Priority Goal (CAP Goal) and improvements to Government mission-support services, enabling the delivery of high-quality outcomes to the American people." OMB asserted that "[i]n the past, agencies took steps to consolidate common mission-support functions internally, and in some cases, to leverage common technology or services offered by other agencies." OMB stated that "[t]he Government endeavors to utilize lessons from previous successes and failures to provide a new, enhanced strategic blueprint for sharing quality services within the Federal enterprise…[and] [i]n addition to improving service quality and performance, private sector experience suggests the potential for significant productivity gains and cost savings over time. " OMB claimed that this intiative has the potential to "realize financial benefits by as much as 5-30 percent" and "[c]ommon mission-support services such as processing hiring transactions or managing Federal finances, travel, and payroll costs taxpayers more than $25 billion annually."

Administration Issues Counterfeit Memorandum

President Donald Trump signed a memorandum "to protect American businesses, intellectual property rights holders, consumers, national and economic security, and the American public from the dangers and negative effects of counterfeit and pirated goods, including those that are imported through online third-party marketplaces and other third-party intermediaries." This directive orders the Department of Homeland Security (DHS) and other agencies to craft a report on how third-party marketplaces and third-party intermediaries are used by counterfeiters to sell fake and knock off goods to U.S. consumers, including recommendations on "appropriate administrative, statutory, regulatory, or other changes, including enhanced enforcement actions, that could substantially reduce trafficking in counterfeit and pirated goods or promote more effective law enforcement regarding trafficking in such goods." Because the Trump Administration considers counterfeiting and piracy to be bigger issues than just the commercial realm, there could be spillover effects on other Administration initiatives.

In the press rollout, the Administration made quite clear that memorandum pertains to companies like Amazon, Alibaba, e-Bay and others, and Assistant to the President and Director of the Office of Trade and Manufacturing Policy Peter Navarro said "[t]his is a warning shot across the bow that it is your job to police these matters, and if you won't clean it up the government will." However, Navarro dismissed questions about whether the memorandum was designed to pressure China and Amazon, two frequent targets of the Administration.

The memorandum also requires investigation into the Department of Defense's efforts to secure its supply chain. The DHS report "should also evaluate the effectiveness of Federal efforts, including

the requirement for certain Federal contractors to establish and maintain a system to detect and avoid counterfeit electronic parts under the Defense Federal Acquisition Regulation Supplement (DFARS) 252.246-7007, as well as steps taken by foreign governments, such as France and Canada, to combat trafficking in counterfeit and pirated goods." This could potentially affect how the Office of Management and Budget (OMB) and General Services Administration (GSA) establish e-Commerce portals required under Section 846 of the FY 2018 National Defense Authorization Act (NDAA), for the Administration has made clear they consider third-party counterfeits a national security problem given the Pentagon's supply chain. The e-Commerce initiative may need to address counterfeits and piracy in response to the report DHS will deliver.

Within seven months, DHS, in conjunction with other stakeholder agencies, must submit a report that includes the following among other elements:

- Analyze available data and other information to develop a deeper understanding of the extent to which online third-party marketplaces and other third party intermediaries are used to facilitate the importation and sale of counterfeit and pirated goods; identify the factors that contribute to trafficking in counterfeit and pirated goods; and describe any market incentives and distortions that may contribute to third-party intermediaries facilitating trafficking in counterfeit and pirated goods.
- Evaluate the existing policies and procedures of third-party intermediaries relating to trafficking in counterfeit and pirated goods, and identify the practices of those entities that have been most effective in curbing the importation and sale of counterfeit and pirated goods, including those conveyed through online third-party marketplaces.
- Identify appropriate administrative, statutory, regulatory, or other changes, including enhanced enforcement actions, that could substantially reduce trafficking in counterfeit and pirated goods or promote more effective law enforcement regarding trafficking in such goods. The report should address the practices of counterfeiters and pirates, including their shipping, fulfillment, and payment logistics, and assess means of mitigating the factors that facilitate trafficking in counterfeit and pirated goods.
- Identify appropriate administrative, regulatory, legislative, or policy changes that would enable agencies, as appropriate, to more effectively share information regarding counterfeit and pirated goods, including suspected counterfeit and pirated goods, with intellectual property rights holders, consumers, and third-party intermediaries.

Other Hearings

"Resourcing DHS' Cybersecurity and Innovation Missions: A Review of the Fiscal Year 2020 Budget Request for the Cybersecurity and Infrastructure Security Agency and the Science and Technology Directorate" – House Homeland Security/Cybersecurity, Infrastructure Protection, and Innovation
"FY2020 Budget Hearing - Cybersecurity and Infrastructure Security Agency" – House Appropriations/Homeland Security

Further Reading

"U.S. cyber official, British telcos to discuss Huawei in London meeting" – *Reuters*
"Dutch intelligence warns of escalating Russian, Chinese cyberattacks in the Netherlands" – *cyberscoop*
"Mueller Findings Raise Election Hacking Fears in States" – *Stateline*
"China making 'rapid progress' on potency of cyber-operations, Pentagon says" – *cyberscoop*

"NSA unmasked more U.S. entities caught in foreign cyber-espionage efforts last year" – *cyberscoop*
"'Cyber event' disrupted U.S. grid networks — DOE" – *E&E News*
"Vodafone denies Huawei Italy security risk" – *BBC*
"As security officials prepare for Russian attack on 2020 presidential race, Trump and aides play down threat" – *The Washington Post*
"No longer clicking: Online ad fraud has fallen in the past year" – *cyberscoop*