Cyber Update
20 March 2019
By Michael Kans

Another Senate Committee Examines GDPR and CCPA

On March 12, the Senate Judiciary Committee held a hearing titled "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation." The committee examined the issue of a federal privacy standard in the context of the existing privacy regime in the European Union (EU), the General Data Protection Regulation (GDPR), and the soon-to-be effective regime in California, the California Consumer Privacy Act (CCPA).

The witnesses appearing before the committee were:
Panel I
Google Senior Privacy Counsel Will DeVries
Californians for Consumer Privacy Chairman Alastair Mactaggart
Intel Security Policy Director and Global Privacy Officer David Hoffman
DuckDuckGo CEO and Founder Gabriel Weinberg
Mapbox Policy Lead Tom Lee

Panel II
American Enterprise Institute Visiting Scholar Roslyn Layton
Center for Democracy and Technology Privacy and Data Project Director Michelle Richardson
University of Arizona Professor of Law Jane Bambauer

Chairman Lindsey Graham (R-SC) remarked that the committee held a joint hearing with the Senate Commerce, Science, and Transportation Committee with Facebook CEO Mark Zuckerberg testifying on privacy issues. He said this hearing focused on what role, if any, Congress should play regarding privacy and social media. Graham said Europe has acted said the hearing would center on whether this is working, helping, or hurting. He said he understood that California was about to pass its own privacy law, set to take effect in January. Graham acknowledged that Senate Commerce has primary jurisdiction over these issues but noted jurisdictional overlaps and that the content piece of these issues belongs to the committee. He said, big picture, he wanted consumers to understand when they sign up for a service that online platforms are monetizing the consumers. He noted online platforms are trying to determine which content to put up and which to take down "with absolutely no guidance from your government." Graham noted that no federal agency is regulating

Michael Kans, Esq. | michaelkans.com | mdk@michaelkanslaw.com |
@michael_kans | michaelkans.blog

online content unlike television stations and newspapers, which can be sued for their content. He asserted there is a lot of bipartisan desire on the committee to do something constructive.

Ranking Member Dianne Feinstein (D-CA) said "I think protecting individual privacy is critical and we must do all we can to give people control over their data." She said that "[c]onsumers are now just becoming aware just how insecure our personal information is with the expansion of smartphones, online services and even appliances in our homes and offices that we regularly use." Feinstein noted that "I represent the state of California, birthplace to some of the most innovative companies in the world at the heart of the Internet revolution…[but] California, though, is also home to some of the most heavily criticized companies for their collection of personal data." She declared that "California is home to the strongest state privacy law in the nation." Feinstein said that "it's my belief that individuals should have as much control as possible over their personal data…[b]ut I also believe affirmative opt-in consent should be the standard, and that's a position I have taken for years – not opt-out." She stated that "[c]ompanies should also be required to protect their customers' personal data with a heightened degree of care, and should be held responsible should that data directly or through cyber breach end up in the wrong hands." Feinstein said "I will not support any federal privacy bill that weakens the California standard…[and] I also believe that any federal legislation should include data breach notification requirements."

DeVries said that "[t]o give detail to [Google's] call for a comprehensive privacy law, we recently published a framework for data protection legislation and provided additional detail in comments to the National Telecommunications and Information Administration." He said that "[a]t its core, comprehensive federal legislation should be risk- and outcomes-based, consistent, adaptable, and work for all types and sizes of businesses and organizations." DeVries said that "[l]egislation should focus on responsible and reasonable data collection and use; transparency; control; security; access, correction, portability, and deletion; adaptability; and accountability." He said that "[i]t should apply to all businesses and organizations that process personal information, and all data that can be used to identify an individual." DeVries said Google encourages "Congress to look to established privacy principles and frameworks, such as the Fair Information Practices Principles (FIPPs), Organization for Economic Co-operation and Development (OECD) Privacy Principles, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and the GDPR to learn what is working, what can be improved, and how to support international interoperability for US-based companies that operate abroad."

Mactaggart stated that "[n]o one law can address the intersection of privacy and technology, any more than one law can address consumer protection, highway

Michael Kans, Esq. | michaelkans.com | mdk@michaelkanslaw.com |
@michael_kans | michaelkans.blog

safety, or food inspection; but CCPA represents a giant step forward, and will help redress the imbalance between consumers and giant businesses that currently exists." He asserted that "I think California took an important step in the right direction, that it will continue to build on this law to ensure that consumers' privacy is protected and respected." Mactaggart said that "I hope Congress will do nothing to undermine that step, as my belief is these new protections have profoundly positive implications for our democratic society going forward." Mactaggart noted "some key facts:

1. 1) In 2017, Google & Facebook took in 63% of US digital ad revenue, which was projected to grow to ~69% in 2019.
2. 2) In 2017 over 90% of the growth in global digital advertising went to Google & Facebook."

Mactaggart claimed that "Google and Facebook (and other large internet companies, though none as much as these two) are collecting unimaginably vast troves of data about consumers, including nearly every email received, every search ever made, every site visited." He added that "[t]hey have the infrastructure in place to track essentially all consumers across all their devices." Mactaggart further asserted that "we think GDPR's 'Notice & Consent' framework is clunky and problematic…[because] [c]onsumers report 'click fatigue' from all the pop-ups, which lose relevance (plus no-one reads the privacy policies, now, any more than they used to)."

Richardson stated that "[p]rivacy legislation must (1) provide individual rights to access, correct, delete, and port personal information; (2) require reasonable data security and corporate responsibility; (3) prohibit unfair data practices, particularly the repurposing or secondary use of sensitive data, with carefully scoped exceptions; (4) prevent data-driven discrimination and civil rights abuses; and (5) provide robust and rigorous enforcement, including additional personnel and original fining authority for the Federal Trade Commission (FTC)."

Bambauer said "I have included with my written testimony a draft bill that codifies much of the regulatory work that the Federal Trade Commission has already done in this area, and expands the FTC's charge to incorporate some of the ideas found in President Obama's draft 2015 Consumer Privacy Bill of Rights and Senator Schatz's proposed Data Care Act." She said that "[t]his draft bill is intended to respond to concerns about the unsupervised expansion of personal data collection and use without promising an unworkable or ultimately harmful degree of user control…[and] [h]ere are the key features that help it respond to the complex problems of data use:

- Duty of Care to avoid unjustified consumer risk or injury. This duty includes, but is not limited to, a requirement to provide notice and consent if the firm will engage in unexpected and material data practices. The failure to provide effective notice for a data practice that would have caused consumers to

Michael Kans, Esq. | michaelkans.com | mdk@michaelkanslaw.com |
@michael_kans | michaelkans.blog

behave differently or choose a different option (including possibly foregoing a product or service) would meet the materiality requirement.

- Duty of Protection to secure personal data from unauthorized access. This duty creates a uniform standard for data security based on industry best practices and clarifies the conditions under which a firm would have to notify consumers about a data breach.
- Duty of Confidentiality limiting the disclosure of personal data to other firms and individuals who are bound by the same duties of care and protection. This duty includes a requirement to reasonably ensure that a recipient of personal data is providing the same level of care and protection by vetting and, if appropriate, auditing the recipient. A company that has reason to know that its partner has violated a duty of care or protection must notify the FTC.
- Federal Trade Commission rulemaking authority to define duties and responsibilities related to personal data practices. The FTC will be authorized, and even required in some cases, to generate and harness expertise and promulgate clear rules of the road for companies that use personal data.
- Preemption of state law to provide predictable and uniform national coverage. This Bill would preempt the California Consumer Protection Act, but would require all U.S. companies to comply with obligations that overlap with the CCPA to some degree.
- Shared enforcement authority between the Federal Trade Commission and state attorneys general. The FTC and State AG offices will share the authority to seek declaratory or injunctive relief and, in cases where a firm had actual knowledge, significant monetary fines for violations of the duties

GAO High-Risk List

The Government Accountability Office (GAO) has released its biennial High-Risk List, and to no great surprise, the GAO flagged a number of cybersecurity, data security, information technology (IT), and acquisitions problems still plaguing federal agencies. However, of note, the GAO removed the DOD's supply chain management from the High-Risk List because of the Pentagon made "made progress on seven actions and outcomes related to monitoring and demonstrated progress that GAO recommended for improving supply chain management." However, on the negative side of the ledger, the GAO again takes the federal government, particularly the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), to task for failing to implement the GAO's many recommendations on IT acquisition and cybersecurity. Additionally, the GAO is calling for Congress to update the Privacy Act of 1974 and the e-Government Act of 2002, and to address privacy and data security at the federal level.

Overall, the GAO noted:

Since GAO's last update in 2017, seven areas improved, three regressed, and two showed mixed progress by improving in some criteria but declining in others. Where there has been improvement in high-risk areas, congressional actions have been critical in spurring progress in addition to actions by executive agencies.
Here are the technology-related items the GAO considers high-risk and their recommendations:

Ensuring the Cybersecurity of the Nation

We have identified four major cybersecurity challenges facing the nation: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address the four major cybersecurity challenges, we identified 10 critical actions the federal government and other entities need to take. These critical actions include, for example, developing and executing a more comprehensive federal strategy for national cybersecurity and global cyberspace; addressing cybersecurity workforce management challenges; and strengthening the federal role in pr
otecting the cybersecurity of critical infrastructure.

We also have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974 and the E-Government Act of 2002, because they may not consistently protect PII. Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect PII in all circumstances of its collection and use throughout the federal government, and may not fully adhere to key privacy principles. However, the relevant revisions to the Privacy Act and the E-Government Act had not yet been enacted as of the date of this report.

Further, we suggested that Congress consider strengthening the consumer privacy framework and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices. However, these suggested changes had not yet been enacted as of the date of this report.

Strengthening Department of Homeland Security Management Functions

Michael Kans, Esq. | michaelkans.com | mdk@michaelkanslaw.com |
@michael_kans | michaelkans.blog

Over the years, we have made hundreds of recommendations related to DHS management functions and many have been implemented. Continued progress for this high-risk area depends primarily on addressing the remaining outcomes. In the coming years, DHS needs to continue implementing its Integrated Strategy for High-Risk Management to show measurable, sustainable progress in implementing corrective actions and achieving outcomes. In doing so, it remains important for DHS to maintain its current level of top leadership support and sustained commitment to ensure continued progress in executing its corrective actions through completion; continue to identify the people and resources necessary to make progress towards achieving outcomes, work to mitigate shortfalls and prioritize initiatives as needed, and communicate to senior leadership critical resource gaps; continue to implement its plan for addressing this high-risk area and periodically provide assessments of its progress to us and Congress; closely track and independently validate the effectiveness and sustainability of its corrective actions, and make midcourse adjustments as needed; and make continued progress in achieving the 13 outcomes it has not fully addressed and demonstrate that systems, personnel, and policies are in place to ensure that progress can be sustained over time.

Improving the Management of IT Acquisitions and Operations

As we have recommended, OMB and covered federal agencies should further implement the requirements of FITARA. OMB will need to provide sustained oversight to ensure that agency actions are completed and the desired results are achieved. Beyond implementing FITARA and OMB's guidance to improve the capacity to address our high-risk area, agencies need to implement our recent recommendations related to improving CIO authorities, as well as past recommendations on improving IT workforce planning practices.
Agencies must establish action plans to modernize or replace obsolete IT investments. Agencies need to implement our recommendations to address weaknesses in their IT Dashboard reporting of investment risk and incremental development implementation.

OMB and agencies should work toward implementing our remaining 456 open recommendations related to this high-risk area. These remaining recommendations include 12 priority recommendations for agencies to, among other things, report all data center consolidation cost savings to OMB, plan to modernize or replace obsolete systems as needed, and improve their implementation of PortfolioStat. OMB and agencies need to take additional actions to (1) implement at least 80 percent of our open recommendations

related to the management of IT acquisitions and operations, (2) ensure that a minimum of 80 percent of the government's major IT acquisitions deliver functionality every 12 months, and (3) achieve at least 80 percent of the over $6 billion in planned PortfolioStat savings.

Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests

The need for action remains in addressing Capacity, Monitoring, and Demonstrated Progress. The Export Enforcement Coordination Center (E2C2) is performing a critical role in coordinating export control enforcement activities, with participation across a wide breadth of federal agencies. However, according to Homeland Security officials, the E2C2 and the intelligence community's lack of formal coordination limits E2C2's effectiveness, stalling its efforts to develop standard operating procedures. Until this coordination occurs, the E2C2 is limited in its ability to realize its full potential to facilitate enhanced coordination and intelligence sharing.

Key agencies have taken necessary steps to reconcile various definitions, regulations, and policies for export controls. If the agencies choose to proceed with consolidation activities initially planned under the 2010 Export Control Reform Initiative, Congressional action will be required. For example, because there are currently separate statutory bases for the Departments of State and Commerce to review and issue export licenses, legislation would be required to consolidate the current system into a single licensing agency.

Cyber Command Budget Request Hearing

Last week, the House Armed Services Committee's Intelligence and Emerging Threats and Capabilities Subcommittee held a hearing titled "Fiscal Year 2020 Budget Request for U.S. Cyber Command and Operations in Cyberspace."

The witnesses testifying before the subcommittee were:

- Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor Kenneth Rapuano
- U.S. Cyber Command Commander and National Security Agency Director General Paul Nakasone

Chairman James Langevin (D-RI) said that "[t]echnology has increased the interconnectedness of our society, and the problems that have come with it will only be solved with interconnected, interdisciplinary approaches." He contended that the

Department of Defense (DOD) "will have to work in new ways with stakeholders from agencies as varied as the Department of Commerce and Department of Education and with non-governmental stakeholders such as private industry and academia." Langevin noted that while the executive branch "will have to work diligently to address and solve the cyber challenges facing the nation….this Administration has taken actions that call into question the seriousness with which it views this emerging domain." He said that notably, the Trump Administration eliminated the Senior Cyber Coordinator position at the National Security Council" and a number of cyber guidance documents the White House has failed to provide to Congress, including the "recent guidance pertaining to operations in cyberspace." Langevin added that "[r]eadiness is especially important in the context of the current strategic landscape, which has evolved significantly over the last year." He said that "U.S. Cyber Command's (CYBERCOM) ability to execute its operations is closely tied to and enabled by its partnership with the National Security Agency (NSA)" and expressed his belief that "it would be premature to split these organizations in the immediate future."

Ranking Member Elise Stefanik (R-NY) stated that "we have seen China and Russia aggressively leverage and integrate cyber, information and communications technologies in a seamless way, while also utilizing top-down, government driven agendas and strategies." She said that "[s]ince our last Cyber Command posture hearing, and over the course of the last year – a lot has happened…[and] [g]iven this, I consider us to be at a major inflection point." Stefanik stated that "[w]e have seen CYBERCOM fully elevated as a functional combatant command, and the force has achieved full operational capability – or FOC." She said that "[r]ecent changes to Presidential cyber policies and strategies – as well as authorities granted in the National Defense Authorization Act - have focused the mission set, yielded impressive operational results, and postured our nation for strategic challenges ahead." Stefanik stated that "while most of our cyber forces are fully capable on paper, they are not fully ready in practice…[and] [s]tandards and capabilities have yet to be defined and understood across each of the Services." She said that "[i]t's worth noting that our military cyber forces are only as good as the technology they depend on; and if we don't concurrently modernize our Information and Communications technologies across the Department - we will continue along with one-hand tied behind our back."

Rapuano said that "[a]lthough the consequences of any single intrusion or action may be limited, in the aggregate these cyber campaigns are a strategic threat to the United States…[and] [c]oordinated malicious cyber activity threatens our prosperity, our democratic institutions, and our national security, including by eroding our military advantage should a conflict occur."

Rapuano said

> For this reason, the DOD Cyber Strategy makes clear that the Department must embrace a proactive and assertive approach during day-to-day competition to deter, disrupt, and defeat these threats. The Department's networks and systems must be made so secure, resilient, and well-defended that we can be assured that the Joint Force will be able to execute its critical missions. During wartime, our forces must be able to operate even while under attack in cyberspace. The DOD Cyber Strategy also directs U.S. cyber forces to target adversary weaknesses, offset adversary strengths, and enhance the effectiveness of the Joint Force. In order to succeed, our cyber forces must be well trained, properly equipped, and provided with the operational latitude and properly delegated authority to prepare the battlefield in advance of potential conflict.

Rapuano stated that "[b]ased on the guidance provided in the National Security Strategy, the National Defense Strategy, and the National Cyber Strategy, the DOD Cyber Strategy sets five clear defense objectives in cyberspace:

- First, the Department must ensure that the Joint Force can achieve its mission in a highly contested cyber domain. The credibility of our military deterrence depends upon making clear that we are prepared to fight and win even against a capable modern adversary. Our systems must be cyber-hardened, resilient, and secure.
- Second, cyber operations must enhance U.S. military advantages and strengthen the Joint Force. Cyber capabilities can increase the speed, reach, and precision of the Joint Force by creating novel, temporary, or reversible effects unmatched by traditional weapons. We are working to expand the scope and capacity of our cyber capabilities and to integrate them into Joint Force planning, exercises, and training.
- Third, we must defend national critical infrastructure from significant foreign malicious cyber activity. This is a new area of emphasis for the Department and reflects the facts that competitors are targeting these assets, and that any large-scale disruption or degradation of national critical infrastructure, not just DOD infrastructure, would be a national security concern. We seek to preempt, defeat, or deter malicious cyber activity targeting national critical infrastructure against a significant cyber incident by defending forward to stop threats before they reach their targets and will support the Department of Homeland Security in fulfilling its responsibility to coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure.
- The fourth objective of the strategy is to secure sensitive DOD information wherever it resides. Nearly every day, the news features a report of a major hacking incident, and states like China are relentlessly seeking to acquire both classified and unclassified data that they can use to gain economic, political, or

military advantage over the United States. Innovation is the seed stock of our future security, and the Department is taking a much stronger approach to protecting that information and the systems on which it resides.
- Fifth and finally, the strategy prioritizes expanding cyber cooperation with our interagency, industry, and international partners to advance our mutual interests, including the protection of infrastructure upon which we rely.

Nakasone said "[o]ur efforts and our continued success depend upon the support of the Congress and of this Committee." He said "[t]hank you in advance for the assistance you are providing us in 2019 as we pursue opportunities in five areas: (1) Supporting strategic competition; (2) Establishing a warfighting ethos across the Command; (3) Improving the readiness of our cyber forces; (4) Enhancing partnerships across government, allies, and the private sector; and (5) Deploying improved operating infrastructure." Nakasone said that "I assess we are seeing what we term corrosive threats, in which malicious cyber actors weaponize personal information, steal intellectual property, and mount influence campaigns…[and] [s]uch measures have had and will have strategic effects on our nation and allies."

Revised IoT Cybersecurity Bill

A revised, narrower version of an Internet of Things (IoT) cybersecurity bill from the last Congress has been reintroduced. However, unlike the versions introduced in the Senate and House in 2017 and 2018, the sponsors in the two chambers have introduced identical bills, indicating that that they have reached agreement on what a bill should look like. The revised bill would place less responsibility on contractors to manage federal IoT cybersecurity and would exclude certain classes of devices not considered IoT by many stakeholders (e.g. computers and smartphones). Yet., despite the broad sponsorship of both bills in terms of the political spectrum, the chairs of the relevant committees have not cosponsored the bill, and a far narrower IoT bill in the last Congress could be sent to the President.

The "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668/S. 734) is a revised, unified version of two similar bills from the 115th Congress of the same title: the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017" (S. 1691) and the "Internet of Things (IoT) Federal Cybersecurity Improvement Act of 2018" (H.R. 7283). The revised bill would apply to virtually all government agencies, including the Department of Defense (DOD), the Intelligence Community (IC) agencies, and independent agencies like the Securities and Exchange Commission (SEC). However, those devices subject to the bill (i.e. "covered devices") are any physical object that can and is connected to the internet and has computer processing capabilities, including collecting, sending, or receiving data. However the category of covered devices is narrower than last year's Senate bill and would explicitly exclude

general-purpose computing devices, including personal computing systems, smart mobile communications devices, programmable logic controls, and mainframe computing systems. However, anyone may ask the Office of Management and Budget (OMB) to modify this definition to include those that do not fall into the definition of covered devices.

The National Institute of Standards and Technology (NIST) would need to complete any current efforts on the cybersecurity of IoT by September 30, 2019. These provisions would work from current NIST IoT efforts, including draft NIST Internal Report 8228 "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" and a draft document "Considerations for a Core IoT Cybersecurity Capabilities Baseline." Also, NIST would need to consider these aspects of IoT cybersecurity: Secure Development; Identity management; Patching; and Configuration management.

Additionally, the bill provides that "[n]ot later than March 31, 2020, the Director of the Institute shall develop recommendations for the Federal Government on the appropriate use and management by the Federal Government of IoT devices owned or controlled by the Federal Government, including minimum information security requirements for managing cybersecurity risks associated with such devices." No later than six months after NIST delivers its federal IoT cybersecurity recommendations, OMB must issue guidelines consistent with those recommendations, covering all federal agencies, including national security and independent agencies. OMB and NIST would need to repeat this process every five years thereafter.

Within six months of enactment, NIST would also need to establish a method by which the federal government could be informed about vulnerabilities in federal IoT and a process for remedying any such weaknesses. Six months later, OMB would follow and issue guidelines for agencies to implement this new process. This new process would affect those entities contracting with the federal government in terms of IoT devices and services, and any such entities failing to comply with OMB's guidelines would be barred by federal agencies from supplying IoT services or devices. By contrast, last year's Senate bill would have required far more disclosure and certification by contractors regarding their IoT, placing the responsibility on them to proactively manage the cybersecurity of federal IoT.

A word about the changes in sponsorship of the bill between this Congress and the last. Unlike last year's Senate bill, Senator Ron Wyden (D-OR) is no longer a sponsor, likely indicating his disagreement with the changes to the Senate bill, which was, as noted, more prescriptive than the House's bill. The sponsors found a different Democrat to introduce the bill, Senator Maggie Hassan (D-NH), thus maintaining the balance of two Republicans and two Democrats with Senators Mark Warner (D-VA),

Cory Gardner (R-CO), Hassan, and Steve Daines (R-MT).

The House bill is sponsored and cosponsored by a number of key cybersecurity stakeholders, including sponsors Robin Kelly (D-IL) and Will Hurd (R-TX), who were the ranking member and chair of the now abolished IT Subcommittee of the House Oversight and Government Reform Committee over the last two years. Representatives Ted Lieu (D-CA), John Ratcliffe (R-TX), Gerry Connolly (D-VA), Mark Meadows (R-NC), and Mark Walker (R-NC), and Ro Khanna (D-CA) are cosponsoring.

However, chairs Bennie Thompson (D-MS) (Homeland Security) and Elijah Cummings (D-MD)(Oversight and Government Reform) are not cosponsoring, which suggests opposition to the bill, but their stances remain to be seen. Likewise, in the Senate, the chair of the Committee through which this bill would need to advance is not a sponsor, and Senator Ron Johnson (R-WI) has been accused by a number of stakeholders of killing cybersecurity bills in the Senate Homeland Security Committee.

Finally, it must be said that Congress could not pass a far more anodyne IoT bill last year, the "Developing Innovation and Growing the Internet of Things (DIGIT) Act" (S. 88), meaning policymakers may not be ready to pass this more expansive bill just yet. However, the agreement on bill language between the two chambers could suggest this bill could be passed.

In August 2017, Warner, Gardner, Wyden, and Daines introduced the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017" (S. 1691) that would require federal agencies to use contract clauses to ensure the security of IoT devices sold to or used by the government by placing the onus on federal contractors to vouch for the security and correction of vulnerabilities of these devices. In their summary of the bill, the Senators claimed the bill "is aimed at addressing the market failure by establishing minimum security requirements for federal procurements of connected devices." If enacted as drafted, the bill may drive the development and proliferation of industry practices to secure and patch IoT in the private sector as well because the federal government is one of the biggest buyers of goods and services.

The legislation requires OMB to "issue guidelines for each executive agency to require" a number of contract clauses for the "acquisition of Internet-connected devices" and establish a process for contractors to disclose known vulnerabilities at the time of placing a bid and asking for a waiver based on a justification for still using the device and any actions that can mitigate or eliminate the vulnerabilities.

Additionally, OMB and NIST would "define a set of conditions" that any devices could meet in order to be procured that do not meet the de facto security standards

that OMB's guidelines on mandatory contract clauses will bring into being. The Department of Homeland Security's former National Protection and Programs Directorate (NPPD) would issue guidelines "for each agency with respect to any Internet-connected device in use of by the United States regarding cybersecurity coordinated disclosure requirements that shall be required of contractors providing such software to the United States Government." Finally, researchers the cybersecurity of IoT devices would receive a liability shield from the "Computer Fraud and Abuse Act" and copyright laws provided such research is conducted in "good faith."

Senators Introduce A Pair of Privacy Bills

Senators Josh Hawley (R-MO) and Edward Markey (D-MA) released their bill (S. 748) "aimed at stopping corporate giants, including social media titans, from targeting and tracking kids online" according to their press release. They claimed that "[a]mong its many improvements, the bipartisan bill updates the Children's Online Privacy Protection Act (COPPA) by prohibiting internet companies from collecting personal and location information from anyone under the age of 13 without parental consent and from anyone ages 13 to 15 without the user's consent."

Hawley and Markey explained that "The legislation strengthens privacy protections specifically for children and minors by:

- Prohibiting internet companies from collecting personal and location information from anyone under 13 without parental consent and from anyone 13 to 15 years old without the user's consent;
- Banning targeted advertising directed at children;
- Establishing a "Digital Marketing Bill of Rights for Teens" that limits the collection of personal information of teens;
- Revising COPPA's "Actual knowledge" standard to a "constructive knowledge" standard for the definition of covered operators;
- Creating an "Eraser Button" for parents and children by requiring companies to permit users to eliminate publicly available personal information content when technologically feasible.
- Establishing a Youth Marketing and Privacy Division at the Federal Trade Commission (FTC);
- Requiring online companies to explain the types of personal information collected, how that information is used and disclosed, and the policies for collection of personal information; and
- Prohibiting the sale of internet connected devices to children and minors unless they meet robust cyber security standards;

- Requiring manufacturers of connected devices to children and minors to prominently display on their packaging a privacy dashboard detailing how sensitive information is collected, transmitted, retained, used, and protected."

Senator John Kennedy (R-LA) unveiled the "Own Your Own Data Act" (S. 806) that would "prohibit the collection of private data by social media companies and grant users the property rights to all of the data that they generate on the internet" as explained in his press release. Broadly speaking, his bill would provide that "[e]ach individual owns and has an exclusive property right in the data that individual generates on the internet under section 5 of the Federal Trade Commission Act." Every person could request and receive their personal data from social media platforms and would be free to enter into licensing agreements allowing a social media company to use the person's personal data.

Estonia Says Russia Will Meddle in EU Elections

Last week, the Estonian Foreign Intelligence Service (Välisluureamet) publicly released its annual assessments of risks against Estonia and Europe for only the fourth time because of the threats posed by Russia and to a lesser extent China. Välisluureamet foresees continued Russian cyber campaigns across a number of cyber-dimensions, including attemtpts to interefere with upcoming European Union (EU) elections. The agency also flagged concerns cited by the United States (U.S.) and ohter allies regarding China's cyber operations and their growing dominance in the hardware and 5G markets.

Välisluureamet asserted that "[t]he main external security threat for Estonia arises from Russia's behaviour, which undermines the international order. The agency contended that "Russia conducts its foreign policy by demonstrating its military force, by using the dependence of other states on Russia's energy carriers, and by conducting cyber attacks and influence operations using false information and other 'soft' tools. Välisluureamet claimed that "Ukraine will be the main target of those measures this year, but Russia will not hesitate to use them even against its ally, Belarus Countries in the European Union and NATO are not fully protected from Russia's aggressive activities, either – it has only been a year since Russia used a chemical weapon on the territory of the United Kingdom."

Välisluureamet stated that "[a]part from the military threat, our intelligence service has to identify and prevent Russia's influence activities in Western countries, the goal of which is to destroy their unity; for example, concerning their attitude to the sanctions imposed on Russia. The agency said that "[t]o achieve that, Russia is prepared to get involved in other countries' domestic policy...[and] [t]he issue of influence activities deserves particular attention this year, as EU member states are

going to elect representatives to the European Parliament." The agency explained that "[t]he world is increasingly analysing the risks arising from the use of Chinese technology and China's investments in other countries' critical infrastructure."

Välisluureamet stated that "[t]he Russian special services' cyber operations and the characteristic masquerading of their attacks caught wider attention in 2018. The agency stated that "[t]he special services' cyber attacks in connection with the Skripal poisoning, the capture of Russian military intelligence (GRU) officers as they were preparing a cyber attack on the Organisation for the Prohibition of Chemical Weapons, data breaches by APT28, a GRU cyber espionage group, during the South Korean Winter Olympics, and Brexit-related phishing e-mails clearly showed that, despite public attention, accusations and sanctions, the Russian special services remain consistently active in cyber espionage."

Välisluureamet observed that

- Most of the cyber and information operations originating from Russia are led by the special services, particularly the FSB and GRU. The methods used are numerous Among the most widely used recent approaches is masquerading as cyber criminals or recruiting actual cyber criminals to do the work.
- Local cyber criminals are also causing problems for Russia itself Fighting cyber crime is the responsibility of the interior ministry's Directorate K and the FSB, both of which cooperate with the private sector, including Kaspersky Lab However, the law enforcement agencies are primarily interested in those who act against Russia's own authorities.
- Russia's malicious cyber activity also involves 'patriotic hackers', who seem unrelated to Russian national interests and special services but always show increased activity during military or geopolitical conflicts where Russia's interests are at stake. The main methods of these patriotic hackers are website defacement and denial-of-service attacks, as well as the dissemination of false information to disrupt nationally and socially important services.

Regarding China, Välisluureamet stated that "cyber operations serving China's national interests have gained wide coverage worldwide. The agency explained that "[s]ecurity breaches or "backdoors" on Chinese IT devices have been identified; malware has been found on mobile devices, computers, and more sophisticated network devices. The Välisluureamet sätted that "Chinese cyber operations have been found to support the efforts of the communist party and the military and involve industrial espionage for the benefit of Chinese technology companies."

Välisluureamet stated that "[s]everal countries (the United States, Australia, New Zealand and others) restrict the use of Chinese technology in national telecommunications solutions due to suspicions that it may be used for intelligence

purposes in the interests of China or a third party." The agency said that "[r]ecognised security threats include the use of Huawei or ZTE security solutions, such as firewalls, which are considered unpredictable and unsafe." Välisluureamet said that "[w]ith Huawei, it has not been possible to verify and the manufacturer has not convincingly proved that it does not rely on the Chinese National Intelligence Law (in force from June 2017), under which "any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of...The state shall protect individuals and organisations that support, cooperate with, and col- laborate in national intelligence work "

Välisluureamet stated that "[t]hus, in China, as in Russia, domestic companies and foreign businesses operating there are required by law to cooperate with the state and its security agencies." The agency stated that "[i]n the assessment of the Estonian Foreign Intelligence Service, these risks have to be carefully analysed in order to avoid dependency that could potentially be a security threat to both the public and private sector."

Warren Wants To Break Up "Big Tech"

Over the weekend, Senator Elizabeth Warren (D-MA) proposed using anti-trust laws to break up large technology companies as part of her campaign to win the Democratic nomination for President. In her blog posting "Here's how we can break up Big Tech," Warren outlined her approach to addressing companies like Google, Amazon, Facebook, and others. Even if Warren does not secure the nomination, her proposals may quickly become the consensus position among most of the Democratic challengers, meaning that the Democratic Party might more fully align itself with those seeking to use anti-trust laws and enforcement to combat what they see as the excesses of the large technology firms.

Warren claimed that "[t]oday's big tech companies have too much power—too much power over our economy, our society, and our democracy." She stated that "[t]hey've bulldozed competition, used our private information for profit, and tilted the playing field against everyone else...[a]nd in the process, they have hurt small businesses and stifled innovation." Warren declared that "I want a government that makes sure everybody—even the biggest and most powerful companies in America—plays by the rules...[a]nd I want to make sure that the next generation of great American tech companies can flourish." She said that "[t]o do that, we need to stop this generation of big tech companies from throwing around their political power to shape the rules in their favor and throwing around their economic power to snuff out or buy up every potential competitor." Warren remarked "[t]hat's why my

administration will make big, structural changes to the tech sector to promote more competition—including breaking up Amazon, Facebook, and Google."

Warren said that "[i]n this tradition, my administration would restore competition to the tech sector by taking two major steps:

- First, by passing legislation that requires large tech platforms to be designated as "Platform Utilities" and broken apart from any participant on that platform.
- Second, my administration would appoint regulators committed to reversing illegal and anti-competitive tech mergers.

Warren conceded that "[o]f course, my proposals today won't solve every problem we have with our big tech companies." She said that "[w]e must give people more control over how their personal information is collected, shared, and sold—and do it in a way that doesn't lock in massive competitive advantages for the companies that already have a ton of our data." Warren added that "[w]e must help America's content creators—from local newspapers and national magazines to comedians and musicians—keep more of the value their content generates, rather than seeing it scooped up by companies like Google and Facebook." She stated that "we must ensure that Russia—or any other foreign power—can't use Facebook or any other form of social media to influence our elections."

Other Hearings and Events

"A New Approach for an Era of U.S.-China Competition" – Senate Foreign Relations
"Securing Federal Networks and State Election Systems" – House Appropriations/ Homeland Security
"Cyber Crime: An Existential Threat to Small Business" – Senate Small Business
"Artificial Intelligence Initiatives within the Department of Defense" – Senate Armed Services/Emerging Threats and Capabilities

Further Reading

"Russian Trolls Shift Strategy to Disrupt U.S. Election in 2020" – *Bloomberg*
"Georgia county pays a whopping $400,000 to get rid of a ransomware infection" – *ZDNet*
"Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Germany" – *The Wall Street Journal* and "Germany asserts independence after U.S. warning on Huawei" – *Reuters*
"Facebook's Data Deals Are Under Criminal Investigation" – *The New York Times*
"Don't break up big tech – regulate data access, says EU antitrust chief" – *TechCrunch*

Michael Kans, Esq. | michaelkans.com | mdk@michaelkanslaw.com |
@michael_kans | michaelkans.blog

"Zuckerberg says he's going all in on private messaging. Facebook's declining user numbers tell us why." – *Washington Post*
"T-Mobile Reveals More Location Data Abuse Following Questions from Senator Wyden" – *Motherboard*
"The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show" – *BuzzFeed News*
"China Gains on U.S. in Highly Cited AI Research" – *The Wall Street Journal*