# Michael Kans' Technology Policy Update
# 19 June 2019
# By Michael Kans, Esq.

**Committee Examines Data Brokers**

The Senate Banking, Housing, and Urban Affairs Committee continued its series of hearings into privacy and data security with a hearing titled "Data Brokers and the Impact on Financial Data Privacy, Credit, Insurance, Employment and Housing." The chair and ranking member continued to state their views that how the privacy of Americans is treated by data brokers and other entities under the Fair Credit and Reporting Act (FCRA) needs to be reexamined in the digital era. Whether this means the committee produces legislation is, at this point, unclear, as is how widely such legislation would sweep. It is possible in the event Congress stalls on broader privacy legislation, the committee produces a bill revising the FCRA to reform the standards and requirements the consumer reporting agencies must meet and explicitly making data brokers and other entities selling, sharing, using, and aggregating consumer data part of the FCRA. Whether the Federal Trade Commission (FTC) would receive additional authority and resources to enforce the FCRA are open questions.

These witnesses testified:

- Government Accountability Office (GAO) Financial Markets and Community Investment Director Alicia Puente Cackley
- World Privacy Forum Executive Director Pam Dixon

Chair Mike Crapo (R-ID) stated that "[a]s a result of an increasingly digital economy, more personal information is available to companies than ever before…[and] I have been troubled by government agencies and private companies' collection of personally-identifiable information for a long time." He remarked that "[t]here have been many questions about how individuals' or groups of individuals' information is collected, with whom it is shared or sold, how it is used and how it is secured." Crapo stated that "[p]rivate companies are collecting, processing, analyzing and sharing considerable data on individuals for all kinds of purposes…[and] [e]ven more troubling is that the vast majority of Americans do not even know what data is being collected, by whom and for what purpose."

Crapo stated that "[t]he Banking Committee has been examining the data privacy issue in both the private and public sectors, from regulators to financial companies to other companies who gather vast amount of personal information on individuals or groups of individuals, to see what can be done through legislation, regulation or by instituting best practices." Crapo stated that "[e]nacted in 1970, the Fair Credit Reporting Act (FCRA) is a law in the Banking Committee's jurisdiction which aims to promote the accuracy, fairness and privacy of consumer information contained in the files of consumer reporting agencies." He said that "[g]iven the exponential growth and use of data since that time, and the rise of entities that appear to serve a similar function as the original credit reporting agencies, it is worth examining how the FCRA should work in a digital economy." Crapo said that "[d]uring today's hearing, I look forward to learning more about the structure and practices of the data broker industry and technology companies, such as large social media platforms; how the data broker industry has evolved with the development of new technologies, and their interaction with technology companies; what information these entities collect, and with whom it is

shared and for what purposes; what gaps exist in federal privacy law; and what changes to federal law, including the FCRA, should be considered to give individuals real control over their data."

Ranking Member Sherrod Brown (D-OH) said that "[t]oday, we're looking at a shadowy industry known as "data brokers..[and] [m]ost of you probably haven't heard of these companies." He stated that "[t]he biggest ones include names like Acxiom, CoreLogic, Spokeo, ZoomInfo, and Oracle…[and] [a]ccording to some estimates, 4,000 of these companies are collecting and selling our private information, but not one of them was willing to show up and speak in front of the committee today." Brown stated that "[t]hese companies expect to be trusted with the most personal and private information you could imagine about millions of Americans, but they're not even willing to show up and explain how their industry works." He asserted that "I think that tells you all you need to know about how much they want their own faces and names associated with their industry." Brown claimed that "[j]ust like in the financial crisis, a group of shadowy players sits at the center of the market, exercising enormous influence over consumers and the economy while facing little or no rules at all." He asserted that "Chairman Crapo and I are committed to shining a light on these companies, and to keeping an unregulated data economy from spiraling out of control." Brown observed that "[j]ust yesterday it was reported that a Department of Homeland Security contractor allowed unauthorized access to photos of travelers and their license plates to be exposed to potential identity thieves." He stated that "[t]he Chairman and I agree that protecting sensitive information like this is timely, and important…[and] I look forward to the witnesses' testimony, and to continuing to work with Chairman Crapo in a bipartisan manner."

Government Accountability Office (GAO) Financial Markets and Community Investment Director Alicia Puente Cackley stated that

> Information resellers (also known as data brokers) are companies that collect and resell information on individuals. Privacy concerns about resellers stem, in part, from consumers not always knowing what personal information is collected and how it is used. Moreover, growing use of the internet, social media, and mobile applications has intensified privacy concerns because these media make it much easier to gather personal information, track online behavior, and monitor individuals' locations and activities.

Puente Cackley explained that

> The scope of consumer privacy protections provided under federal law has remained narrow in relation to (1) individuals' ability to access, control, and correct their personal data; (2) collection methods and sources and types of consumer information collected; (3) new technologies; and (4) some regulatory authorities.

Puente Cackley asserted that

> The current privacy framework does not fully address new technologies such as facial recognition technology, privacy issues raised by online tracking and mobile devices, and activities by financial technology firms. The original enactment of several federal privacy laws predates these trends and technologies. But in some instances existing laws have been interpreted to apply to new technologies. For example, FTC has taken enforcement actions under COPPA and revised the statute's implementing regulations to account for smartphones and mobile applications.

Puente Cackley claimed that "new technologies have vastly changed the amount of personal information private companies collect and how they use it…[b]ut our current privacy framework does not fully address these changes." She stated that "[l]aws protecting privacy interests are tailored to specific sectors and uses…[a]nd, consumers have little control over how their information is collected, used, and shared with third parties for marketing purposes." Puente Cackley stated that "[a]s a result, current privacy law is not always aligned with the Fair Information Practice Principles, which the Department of Commerce and others have said should serve as the foundation for commercial data privacy…[and] [t]hus, the privacy framework warrants reconsideration by Congress in relation to consumer interests, new technologies, and other issues.

World Privacy Forum Executive Director Pam Dixon offered "four core observations and two solutions:

1. Credit scores and predictions are being sold that are not regulated by the FCRA,
2. The technology environment is facilitating more scores being used in more places in consumers' lives, and not all uses are positive,
3. These scores are created without due process for consumers,
4. These scores can cause consumers exceptional harm."

She stated that "[t]herefore, Congress must:

1. Expand the Fair Credit Reporting Act to regulate currently unregulated financial scores that affect consumers,
2. Enact a standards law that will provide due process and fair standard setting in the area of privacy."

Dixon stated that "[b]y doing these things, Congress will protect consumers and allow them to act to fill in gaps where privacy harms are occurring, along with other stakeholders."

**Deep Fakes Hearing**

The House Intelligence Committee held a hearing titled "The National Security Challenge of Artificial Intelligence, Manipulated Media, and 'Deepfakes'" last week with testimony from:

- University of Maryland School of Law Professor Danielle Citron
- OpenAI Policy Director Jack Clark
- University at Buffalo Professor David Doermann
- German Marshall Fund Senior Fellow Clint Watts

Chair Adam Schiff (D-CA) noted that "[a]dvances in artificial intelligence (AI) and machine learning have led to the emergence of advanced digitally doctored types of media, so-called "deepfakes,"that enable malicious actors to foment chaos, division or crisis and they have the capacity to disrupt entire campaigns, including that for the presidency." He asserted that "[r]apid progress in artificial intelligence algorithms has made it possible to manipulate media – video, imagery, audio, and text – with incredible, nearly imperceptible results." Schiff claimed that "[w]ith sufficient training data, these powerful deepfake-generating algorithms can portray a real person doing something they never did, or saying words they never uttered." He added that "[t]hese tools are readily available and accessible to both experts and novices alike, meaning that attribution of a deepfake to a specific author – whether a hostile intelligence service or a single Internet troll – will be a constant challenge."

Schiff stated that "[t]hinking ahead to 2020 and beyond, one does not need any great imagination to envision even more nightmarish scenarios that would leave the government, the media, and the public struggling to discern what is real and what is fake:

- A state-backed actor creates a deepfake video of a political candidate accepting a bribe, with the goal of influencing an election;
- An individual hacker claims to have stolen audio of a private conversation between two world leaders, when in fact no such conversation took place;
- A troll farm uses text-generating algorithms to write false or sensational news stories at scale, flooding social media platforms and overwhelming journalists' ability to verify, and users' ability to trust what they are reading.

He contended that "[w]hat enables deepfakes and other modes of disinformation to become truly pernicious is the ubiquity of social media, and the velocity at which false information can spread…[and] [w]e got a preview of what that might look like recently when a doctored video of Speaker Nancy Pelosi went viral on Facebook, receiving millions of views in the span of 48 hours." Schiff declared that "[n]ow is the time for social media companies to put in place policies to protect users from misinformation, not in 2021 after viral deepfakes have polluted the 2020 elections…[because] [b]y then, it will be too late."

Devin Nunes (R-CA) stated "[a]rtificial intelligence and deepfake technology present a growing threat to our national security, and I look forward to the discussion…[and] [g]iven that we have a lot to cover today, and votes will be called relatively early today, I yield back."

Citron explained that "[n]o criminal or civil liability regime specifically addresses the creation or distribution of deep fakes." She stated that "[a] ban on deep fake technology would not be desirable…[and] [d]igital manipulation is not inherently problematic." She explained that "[t]here are pro-social uses of the technology…[and] [d]eep fakes exact significant harm in certain contexts but not in all." Citron stated that "[e]xisting civil and criminal laws would address certain deep fakes." She stated that "[t]ort law would provide redress for some deep-fake scenarios…[and] [d]eep-fake creators could be sued for defamation where falsehoods are circulated recklessly in the case of public figures or officials or negligently in the case of private individuals." Citron said that "[t]he "false light" tort—recklessly creating a harmful and false implication about someone in a public setting—likewise has potential for certain cases." She claimed that "[s]ubjects of deep fakes may be able to bring claims for intentional infliction of emotional distress, which requires proof of 'extreme and outrageous conduct.'"

Citron stated that "[p]ublic figures could bring "right of publicity" claims if defendants generate financial gain from the fakes." She said that "[c]riminal law offers limited avenues for deterrence and punishment…[and] [a] handful of states criminalize impersonations that cause certain injuries." Citron stated that "[i]n a few jurisdictions, creators of deep fakes could face charges for criminal defamation if they posted videos knowing they were fake or if they were reckless as to their truth or falsity." She stated that "[i]f perpetrators post deep fakes in connection with the persistent targeting of individuals, they might be prosecuted for violating the federal cyberstalking law as well as analogous state statutes."

Citron stated that "federal immunity should be amended to condition the immunity on reasonable moderation practices rather than the free pass that exists today." She contended that "[t]he current interpretation of Section 230 leaves platforms with no incentive to address destructive deep-fake content…[and] [t]o be sure, there are platforms that do not need civil liability exposure to combat

such obvious harms; market pressures and morals in some cases are enough." Citron added that "market pressures and morals are not always enough, and they should not have to be."

Clark stated that "[i]t seems like the following things are true:

- It is going to become easier to create increasingly convincing fake media as AI technology advances.
- AI technology is a general-purpose, omni-use technology, so it is challenging to call for specific technical controls to mitigate against specific outputs (e.g., deep fakes), without stifling broader innovation and research.
- Controlling the diffusion of technical AI capabilities is difficult-by-default due to incentives baked into the AI development community (and broader software development community).
- Many of the sources of control are not so much technical, as opposed to the systems that surround the technology. (For instance, one way to defend against people using AI-synthesized voices in telemarketing scams is to simply make it harder for criminals to spoof phone numbers).

Clark remarked that "[g]iven these traits, we believe we need three types of interventions: technical, institutional, and political." He stated that:

- By technical, we mean there are a variety of specific technical interventions which can be made to help us detect use of these technologies.
- By institutional, we mean there are things that can be done at the level of major technology platforms which could help to provide society with the ability to respond to large-scale fakemedia events.
- By political, we mean that some interventions will occur at the level of government(s) taking actions, and these actions should likely include a mixture of building capacity in federal government, increasing dialogue between government actors and technical actors.

Doermann stated that "[t]here is no easy solution, and it will likely get much worse before it gets better…[and] [y]et we have to continue to do what we can:

- We need to get tools and processes in the hands of individuals, rather than relying completely on the government or social media platforms to police content. If individuals perform the "sniff test" and media fails, they should have ways to verify or prove it.
- We need to continue to work toward being able to apply "automated" detection and filtering capabilities at scale. It is not sufficient to only analyze questioned content after the fact. We need to be able to apply detection capabilities at the front end of the distribution pipeline. And even if we don't prevent it from appearing, it should come with the appropriate warnings that suggest that it is not real or not authentic.
- We need to continue to put pressure on our social media companies so that they realize that the way their platforms are being abused is not acceptable. And that they must do all they can to address todays issues, and not allow things to get any worse.

Watts claimed that "[t]he U.S. government should rapidly develop policies to promote appropriate use of artificial intelligence in media content creation and support technological development to verify the authenticity of video and audio content:

- First, Congress should implement legislation prohibiting U.S. officials, elected representatives and agencies from creating and distributing false and manipulated content. The U.S. government must always be the purveyor of facts and truth to its constituents assuring the effective administration of democracy via productive policy debate from a shared basis of reality.

- Second, policymakers should work jointly with social media companies to develop standards for content accountability. Protecting account anonymity for those producing authentic content and exercising their free speech rights should be the goal for Western democratic societies. But there is no public good in permitting the proliferation of inauthentic content from inauthentic accounts. For those producing and promoting inauthentic synthetic media from authentic accounts, they should be held responsible for their content and any violations of platform terms of service.
- Third, the U.S. government should partner with the private sector to implement digital verification signatures designating the date, time and physical origination of content. Time stamping will help information consumers understand the authenticity of content and will help ensure a collective public reality.
- Fourth, social media companies should enhance their labeling of synthetic content across platforms and work as an industry to codify how and when manipulated or faked content should be appropriately marked. Not all synthetic media is nefarious in nature. But, information consumers should be able to determine the source of information and whether it is an authentic depiction of people and events.
- Fifth, the U.S. government, from a national security perspective, should maintain intelligence on adversaries capable of deploying 'Deepfake' content or the proxies they employ to conduct such disinformation. The Departments of Defense and State should develop immediate response plans for 'Deepfake' smear campaigns and 'Deepfake' inspired violent mobilizations over seas in an attempt to mitigate harm to U.S. personnel and interests.
- Sixth, public awareness of 'Deepfakes' and its signatures will greatly assist in tamping down attempts to subvert U.S. democracy and incite violence. Public-private partnerships could develop educational materials regarding 'Deepfakes' which could then be delivered to Americans via the Internet and social media. Public awareness might likely be the best inoculation to the ill effects of fake audio and video content.

**DHS Cyber Hunt Teams Bill Moves**

Last week, the House took up and passed the "DHS Cyber Incident Response Teams Act of 2019" (H.R. 1158), as amended, by voice vote. H.R. 1158 would require the Cybersecurity and Infrastructure Security Agency's (CISA) National Cybersecurity and Communications Integration Center (NCCIC) to "maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

- Assistance to asset owners and operators in restoring services following a cyber incident.
- The identification of cybersecurity risk and unauthorized cyber activity.
- Mitigation strategies to prevent, deter, and protect against cybersecurity risks.
- Recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate.
- Such other capabilities as the Under Secretary…determines appropriate."

Additionally, NCCIC must "continually assess and evaluate the cyber incident response teams and their operations using robust metrics" and may "include cybersecurity specialists from the private sector on cyber hunt and incident response teams."

In the Committee Report, the House Homeland Security Committee explained

> DHS's NCCIC currently utilizes cyber incident response expertise in several ways. The United States Computer Emergency Readiness Team (US–CERT), operated within the NCCIC, brings

> advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. USCERT develops timely and actionable information for distribution to Federal departments and agencies, state and local governments, private sector organizations, and international partners. The critical mission activities of US–CERT's include: providing cybersecurity protection to Federal civilian executive branch agencies; responding to incidents and analyzing data about emerging cyber threats; and collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.

The committee added

> The NCCIC's cyber incident teams, known as Hunt and Incident Response Teams (HIRT), provide onsite incident response, free of charge, to organizations that require immediate investigation and resolution of cyber-attacks. These teams provide DHS's front-line response for cyber incidents and proactively hunting for malicious cyber activity. Upon notification of a cyber incident, HIRT will per-form a preliminary diagnosis to determine the extent of the com-promise. When requested, HIRT can deploy a team to meet with the affected organization to review network topology, identify infected systems and collect other data as needed to perform thorough follow on analysis. They also can provide mitigation strategies and assist asset owners and operators in restoring service and pro-vide recommendations for improving overall network and control systems security.

A related bill has been marked up and reported out of the Senate Homeland Security and Governmental Affairs Committee, the "DHS Cyber Hunt and Incident Response Teams Act of 2019" (S. 315), that would charge NCCIC and CISA with substantially the same missions. Yet, it is unclear when, or if, the Senate will take up either bill.

**Committee Finishes Work On Appropriations; Last Two Bills Have Cyber Provisions**

On June 11, the House Appropriations Committee marked up and reported out the FY 2020 Homeland Security Appropriations Act, and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) would receive $2.016 billion for FY 2020, a boost of $334 million above its FY 2019 funding level and $408 million above the Administration's budget request. The draft Committee Report contained a number of cyber-related passages:

- *Cybersecurity Briefings.*—The Committee directs CISA to continue providing the semiannual National Cybersecurity Protection System (NCPS) program and CDM program briefing described in House Report 116–9. In addition to those requirements, the briefing shall also include a detailed description of the cybersecurity services that CISA provides or is planning to provide to agencies at no-cost, a reduced cost, or under a shared-services model. Further, in collaboration with the Office of Management and Budget (OMB) and other agencies, as needed, this briefing shall also pro- vide a full description of the CDM and NCPS capabilities currently deployed; the gaps remaining; and funding levels by agency, for the prior fiscal year, the current fiscal year, and the budget year for each capability.
- *Cybersecurity Workforce.*—The Committee continues to be concerned about the growing cybersecurity workforce gap in our country. Not later than 120 days after the date of enactment of this Act, the Committee directs CISA, in collaboration with OMB, the Office of Personnel Management, and other agencies and organizations with equities in this issue, to update the Committee on the deliverables required in the "Solving the Federal

Cybersecurity Workforce Shortage" proposal and the Executive Order on America's Cybersecurity Workforce. These activities cover the following focus areas: K–12 through post-secondary education; training and development programs; recruitment strategies; and competitiveness challenges facing public sectors. The update should address how these activities will create pathways to train and develop individuals seeking to enter the cybersecurity field, particularly those who may currently be underrepresented in the field, including veterans, minorities, and women. It should also include a description of the roles and responsibilities of each federal agency that currently pro- vides resources in this area, together with a funding history for fiscal years 2017 through 2019 and their respective funding requests for fiscal year 2020.

- *Election Infrastructure Security Initiative (EISI)*.—The recommendation includes $24,071,000 for EISI, as requested. In preparation for the 2020 elections, the Committee encourages CISA to improve National Cybersecurity and Communications Integration Center (NCCIC) operational efficiency and coordination, especially with National Guard units that have advanced cybersecurity skills. This effort should include process improvements and increased capability to support training, risk assessments, and incident response or other needs of state and local governments.
- *Federal Cybersecurity*.—The recommendation includes an in- crease above the request of $17,000,000 to accelerate data protection and dashboard deployment for the CDM program, of which not less than $3,000,000 shall be for endpoint protection. The Committee directs CISA to continue pilot programs within CDM that extend incident detection and prevention to federal endpoints. The pilot programs should focus on leveraging emerging technologies like cloud-based endpoint protection platform solutions, including detection and response, that can promote enhanced defenses and continuous threat hunting across the federal enterprise. The Committee also encourages CISA to evaluate the efficacy and feasibility of incorporating "break and inspect" capabilities into the CDM architecture to address challenges associated with inspecting and securing encrypted network traffic at scale without a material degradation in performance.
- The Committee is concerned with the security implications of an increasingly modern federal workforce, which includes more remote employees, enhanced mobility, and an increased focus on cloud technologies. CISA is directed to brief the Committee not later than 180 days after the date of enactment of this Act on a detailed plan to modernize CDM and NCPS to ensure they remain operationally effective given changing trends in technology, the federal work- force, threats, and vulnerabilities. The briefing shall include: (1) a long-term, strategic vision for the program to ensure that CDM and NCPS capabilities continue to develop and evolve in an agile manner to address contemporary technology use and vulnerabilities and combat emerging cybersecurity threats; (2) an assessment of whether emerging private sector technologies that focus on securing endpoints could integrate with existing program capabilities to enhance the overall effectiveness of CDM and NCPS; and (3) preliminary results from all CDM and NCPS-related pilot programs.

The Committee also marked up and reported out the FY 2020 Financial Services and General Government appropriations act, and in the Committee Report, the committee highlighted cybersecurity funding and provisions:

- Election Security.—The U.S. democratic process is under attack— and the country's patchwork of voting systems is woefully under-prepared to withstand efforts by sophisticated nation-states to hack the election process and influence election outcomes. State and local election officials lack the necessary tools and funding to re-place antiquated voting machines, secure voter registration data-bases and electronic pollbooks that are

vulnerable to hackers, conduct cybersecurity training for election officials and poll workers, perform post-election audits to validate election results, or implement other necessary efforts to ensure the integrity of the election process. The Committee recommends $600,000,000 for Election Security Grants to augment efforts by state and local election officials to improve the security of elections for Federal office. The recommendation also includes $16,171,000 for the Election Assistance Commission, an increase of $6,971,000 above fiscal year 2019, to ensure the agency is appropriately resourced to execute its vital mission to assist states in the administration of Federal elections.

- The bill requires States to use payments to replace direct-recording electronic (DRE) voting machines with voting systems that re-quire the use of an individual, durable, voter-verified paper ballot, marked by the voter by hand or through the use of a non-tabulating ballot marking device or system, and made available for inspection and verification by the voter before the vote is cast and counted. Funds shall only be available to a State or local election jurisdiction for further election security improvements after a State has submitted a certification to the EAC that all DRE voting machines have been or are in the process of being replaced. Funds shall be available to States for the following activities to improve the security of elections for Federal office: implementing a post-election, risk-limiting audit system that provides a high level of confidence in the accuracy of the final vote tally; maintaining or upgrading election-related computer systems, including voter registration systems, to address cyber vulnerabilities identified through DHS scans or similar assessments of existing election systems; facilitating cyber and risk mitigation training for State and local election officials; implementing established cybersecurity best practices for election systems; and other priority activities and investments identified by the EAC, in consultation with DHS, to improve election security. The EAC shall define in the Notice of Grant Award the eligible investments and activities for which grant funds may be used by the States. The EAC shall review all proposed investments to ensure funds are used for the purposes set forth in the Notice of Grant Award. The bill also requires that not less than 50 percent of the payment made to a State be allocated in cash or in kind to local government entities responsible for the administration of elections for Federal office.
- Cybersecurity.—The President's budget requested an increase in funding for the Office of Critical Infrastructure Protection (OCIP) of nearly 140 percent. The Committee recognizes the need to protect the financial services sector and its customers from the devastating effects of cyberattacks and supports efforts by both industry and government to mitigate this threat. However, it is unclear how the requested funding will further this goal. Therefore, the Committee recommendation does not include the proposed increase of $7,700,000. OCIP is directed to submit a report to the Committee within 60 days of the date of enactment of this Act on its collaborative efforts with the financial services sector to improve cybersecurity controls and safeguards. The report should include proposed ways to enhance these efforts, including estimated costs for each discrete activity, and a description of how these efforts will produce measurable improvements.
- Continuous Diagnostics and Mitigation (CDM) Solutions.—The Committee is aware that the GSA Office of Inspector General has identified the need to improve the cybersecurity posture within GSA encompassing sensitive data and control systems. The Committee directs GSA, within 120 days of enactment of this Act, to report on the acceleration of adoption of CDM solutions to better secure its information assets and data.
- Enterprise Infrastructure Solutions.—GSA plays a critical role in assisting Federal agencies with the acquisition of telecom services in an efficient, timely, and cost-effective manner. While the Committee understands the challenges Federal agencies face transitioning telecommunication services from one set of contracts to another, the Committee believes it is

important for the GSA to effectively apply lessons learned from prior transitions. According to the GAO's December 5, 2013 Report, "TELECOMMUNI-CATIONS: GSA Needs to Share and Prioritize Lessons Learned to Avoid Future Transition Delays," GAO–14–63, in prior tele-communications transitions, delays in transitioning away from dated contract vehicles resulted in missed savings opportunities, increased transition costs, and narrower ranges of products and services. GSA's Enterprise Infrastructure Solutions (EIS) contract presents Federal agencies with opportunities to transition existing services to a more modern contract vehicle that offers significant savings and the ability to choose a provider that offers seamless support, a nationwide footprint, and the capability to offer services that are not limited to a single underlying carrier's network or product offering. The Committee is aware that EIS is structured to maximize competition by providing Federal agencies with the opportunity to receive best value by logically grouping together relevant services in multiple fair opportunity task orders as opposed to limiting competition by awarding unrelated services to a single service provider that provides the broadest array of products and services. To ensure a timely and efficient transition to EIS, the Committee directs GSA to instruct each agency to adopt an up-dated transition management plan and an integrated transition time line, as recommend by GAO. Further, the Committee directs GSA to provide a report, no later than 60 days following enactment of this Act, detailing steps taken to ensure a timely and efficient transition to EIS that maximizes competition, efficiencies, and tax-payer savings as described above.

**GAO Reports On IT and Identity Proofing**

In two reports requested by Members of Congress, the Government Accountability Office (GAO) shined lights on the federal government's identity proofing systems and legacy information technology dating back to the late 1960s and early 1970s.

The GAO examined the federal government's use of consumer reporting agencies (CRA) to either verify or help verify the identity of people seeking benefits and services in light of the massive 2017 Equifax breach. The GAO looked at six civilian agencies and found that two have transitioned to remote identity proofing processes while the other four still rely on knowledge-based verification. However, both processes rely, in varying degrees, on the CRAs. The GAO also found that the National Institute of Standards and Technology's (NIST) 2017 guide on digital identities does not provide federal agencies with the information necessary for them to use alternatives to knowledge-based proofing. Additionally, the GAO faulted the Office of Management and Budget (OMB) for failing to set government-wide reporting standards to better ascertain the state of the federal's government's efforts to revamp and strengthen identity proofing. In late May, OMB released a memorandum to revise how the federal government's identity, credential, and access management procedures, and GAO remarked of the draft version that it did not contain language on "secure remote identity proofing processes."

The report was requested by Senate Finance Committee Ranking Member Ron Wyden (D-OR), the Senate Banking, Housing, and Urban Affairs Committee's Financial Institutions and Consumer Protection Committee Subcommittee Ranking Member Elizabeth Warren (D-MA), and the House Oversight and Reform Committee Chair Elijah Cummings (D-MD) and Ranking Member Jim Jordan (R-OH). These Members were concerned, in part, about how the sprawling Equifax breach of 145 million Americans' sensitive information might be used to obtain benefits, services, or other

information by fraud. In 2018, the GAO noted that criminals used the personally identifiable information (PII) of thousands of people to defraud the Internal Revenue Service (IRS) of tax returns.

However, despite the requesters of the report possessing positions and stature that would enable them to push for legislative changes, statutory fixes are not immediately apparent. The GAO conceded that OMB already possesses the authority to institute information security standards under the "Federal Information Security Modernization Act of 2014" (FISMA) (P.L. 113-283).

The GAO stated that

> The six agencies that we reviewed rely on a variety of remote identity proofing techniques to help ensure that the individuals who enroll for federal benefits and services are who they claim to be. Several of the selected agencies use knowledge-based verification processes that rely on CRAs to pose questions to individuals and check their answers as a way of verifying their identities before granting them enrollment in a federal benefit or service. However, given recent breaches of sensitive personal information, these agencies face risks because fraudsters may be able to obtain and use an individual's personal information to answer knowledge-based verification questions and successfully impersonate that individual to fraudulently obtain federal benefits and services.

The GAO explained that

> Two agencies we reviewed, GSA and IRS, recently implemented remote identity proofing processes for Login.gov and Get Transcript that allow individuals to enroll online without relying on knowledge-based verification. However, four agencies (CMS, SSA, USPS, and VA) were still using knowledge-based verification to conduct remote identity proofing. Moreover, none of the four agencies have developed specific plans to eliminate knowledge-based methods from their processes. Without such plans, these federal agencies and the individuals that rely on such processes will remain at risk for identity fraud.

The GAO concluded

> NIST has issued technical guidance regarding remote identity proofing, but it may not be sufficient to help ensure that federal agencies adopt more secure methods. NIST's guidance does not provide direction on how agencies can adopt more secure alternatives to knowledge-based verification while also addressing issues of technical feasibility and usability for all members of the public. In addition, OMB has not issued guidance setting agency reporting requirements that OMB could use to track implementation of more secure processes across the federal government. Without additional guidance, federal agencies are likely to continue to rely on risky knowledge-based verification that could be used to fraudulently gain access to federal benefit programs and services.

The GAO also released a report on modernizing legacy information technology (IT) requested by House Members who have been focused on the federal government's information technology (IT) and information security. The GAO looked at the "10 most critical federal legacy systems in need of modernization" and found the agencies did not have complete plans to modernize these systems. Moreover, the GAO identified those factors that have allowed agencies to best modernize legacy IT in the past. The report was requested by House Oversight and Reform Chair Elijah Cummings (D-MD), Ranking Member Jim Jordan (R-OH), the Government Operations Subcommittee Chair Gerry

Connolly (D-VA) and Ranking Member Mark Meadows (R-NC), and Representatives Will Hurd (R-TX) and Robyn Kelly (D-IL). Given the pedigree of these Members with respect to legislating on IT and information security, this request may point to an area of federal systems on which they want to legislate or exert pressure to affect changes.

Specifically, these Members asked the GAO to

> (1) identify the most critical federal legacy systems in need of modernization and evaluate plans for modernizing them, and
> (2) identify examples of legacy system modernization initiatives in the last 5 years that agencies considered successful.

By way of background, the GAO explained

> According to the President's Budget, the federal government plans to spend over $90 billion in fiscal year 2019 on information technology (IT). Of this amount, the government plans to spend about 80 percent on the operations and maintenance of existing IT investments, including aging (also called legacy) systems. However, federal legacy systems are becoming increasingly obsolete. In May 2016, we reported that many of the government's IT investments used outdated software languages and hardware parts that were unsupported. We also reported instances where agencies were using systems that had components that were at least 50 years old or the vendors were no longer providing support for hardware or software. As they age, legacy systems can become more expensive to maintain, more exposed to cybersecurity risks, and less effective in accomplishing their intended purpose.

The GAO stated that "[e]ach of the 24 Chief Financial Officers Act agencies identified their agency's most critical legacy systems in need of modernization...a total of 65 such systems." The GAO added that "[t]he agencies also identified various attributes of the legacy systems, including the systems' age, hardware age, system criticality, and security risk." Appendix II charts the agencies responses regarding their most critical legacy systems, and Appendix III provides profiles of each of the 10 most critical systems without naming them. Here is the chart GAO included in the report:

**Table 1: The 10 Most Critical Federal Legacy Systems in Need of Modernization**

| Agency | System name[a] | System description[a] | Age of system, in years | Age of oldest hardware, in years | System criticality (according to agency) | Security risk (according to agency) |
|---|---|---|---|---|---|---|
| Department of Defense | System 1 | A maintenance system that supports wartime readiness, among other things | 14 | 3 | Moderately high | Moderate |
| Department of Education | System 2 | A system that contains student information | 46 | 3 | High | High |
| Department of Health and Human Services | System 3 | An information system that supports clinical and patient administrative activities | 50 | Unknown[b] | High | High |
| Department of Homeland Security | System 4 | A network that consists of routers, switches, and other network appliances | Between 8 and 11[c] | 11 | High | High |
| Department of the Interior | System 5 | A system that supports the operation of certain dams and power plants | 18 | 18 | High | Moderately high |
| Department of the Treasury | System 6 | A system that contains taxpayer information | 51 | 4 | High | Moderately low |
| Department of Transportation | System 7 | A system that contains information on aircraft | 35 | 7 | High | Moderately high |
| Office of Personnel Management | System 8 | Hardware, software, and service components that support information technology applications and services | 34 | 14 | High | Moderately low |
| Small Business Administration | System 9 | A system that controls access to applications | 17 | 10 | High | Moderately high |
| Social Security Administration | System 10 | A group of systems that contain information on Social Security beneficiaries | 45 | 5 | High | Moderate |

Key:

Agencies reported the system criticality and security risk on a scale of 1 to 5 (with 5 being the most critical and the highest risk).

Low-1: According to the agency, system has low security risk or criticality.

Moderately low-2: According to the agency, system has moderately low security risk or criticality.

Moderate-3: According to the agency, system has moderate security risk or criticality.

Moderately high-4: According to the agency, system has moderately high security risk or criticality.

High-5: According to the agency, system has high security risk or criticality.

Source: GAO analysis of agency data. | GAO-19-471

[a]Due to sensitivity concerns, we substituted a numeric identifier for the system names and only provided general details.

[b]The agency stated that the system's hardware had various refresh dates and that it was not able to identify the oldest hardware.

[c]The agency stated that the majority of the network's hardware was purchased between 2008 and 2011.

Almost all of the systems are rated as being very important to the agencies with some being over 50 years old. Incidentally, in a footnote, the GAO noted "[t]he 10 agencies with the most critical legacy systems in need of modernization are the Departments of Defense, Education, Health and Human Services, Homeland Security, the Interior, the Treasury, and Transportation; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration."

GAO also reviewed previous modernizations of legacy systems that had gone well. GAO stated that "[t]he five agencies attributed the success of their modernization initiatives to various factors, including:

- using automated technologies to examine programming code and perform testing (DOD and Treasury);
- testing the system thoroughly (SSA and Treasury);
- actively engaging the end users and stakeholders throughout the modernization process (SSA and Treasury);

- cultivating a partnership between industry and government (DOD);
- following management practices on change and life cycle management (Education);
- developing and implementing an enterprise-wide cost collection and data analysis process for commodity IT to track and measure progress against consolidation, optimization, and savings targets (DHS);
- creating an interface that was consistent across systems (SSA);
- having strong executive leadership and support (Treasury); and
- using agile principles to facilitate the team's ownership of the project (Treasury)."

Of course, keeping in mind the Members who requested the report, the question becomes whether this presents another venue from which to legislate better IT and information security for federal agencies. Yet, most of the practices for successful modernizations turned up by GAO are well-known and have been mandated in various forms through previous pieces of legislation. So while a bill to refine the federal government's IT and information security may not result from this report, it is very likely the House Oversight and Reform Committee will be using these findings to push agencies to update legacy systems in the most efficient ways. Whether this is through behind the scenes pressure and/or hearings remains to be seen.

**Federal Privacy Legislation Hits Roadblock In House**

Following recent comments by key Senate stakeholders that negotiations on federal privacy legislation may have stalled in that body, there were public remarks that similar talks in the House may also be at an impasse over a new issue: whether the Federal Trade Commission (FTC) would need a new Privacy Division to enforce a privacy statute. The House Energy & Commerce Committee's Consumer Protection & Commerce Subcommittee Chair Jan Schakowsky (D-IL) remarked that "[a]t this point I think we will not be calling for a separate independent agency, but we will be calling for a division within the Federal Trade Commission." Yet, her Republican counterpart, Ranking Member Cathy McMorris Rodgers (R-WA) remarked "I agree that the FTC should be the cop on the beat when it comes to enforcement of privacy standards, but I'm focused on helping consumers through limited and specific jurisdiction of the FTC, not through creating even more bureaucracy." Yet, Schakowsky made clear that Democratic efforts to work with the minority will only go so far: "[o]bviously it would be a great thing if we could do it with the Republicans…[but] [w]e want to, plan to, with or without them."

The Members on the Senate Commerce, Science, and Transportation Committee working together on privacy legislation have hit impasses regarding preemption of state statutes and whether consumers will have a private right of action against entities that violate their privacy rights. It is possible that the issue of whether the FTC would have a Privacy Division has also split Members, too.

**IOT Bill Advances**

The House Oversight and Reform Committee marked up and reported out the "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668) after adopting an amendment in the nature of a substitute that narrowed the scope of the bill and is more directive than the bill initially introduced in March. While there is a Senate bill, it is not clear what the Senate sponsors think of the changes in the bill despite a markup scheduled for this week.

In March, the House and Senate cosponsors of competing IoT bills in the last Congress reach agreement on a bill and introduced identical bills. The "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668/S. 734) represented 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). In general, this bill seeks to leverage the federal government's ability to set standards through acquisition processes to ideally drive the development of more secure IoT across the U.S. The stakeholders are responding to the security risks presented by weak or nonexistent security for IoT as seen in a number of major malware attacks. The legislation would require the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to work together to institute standards for IoT owned or controlled by most federal agencies. These standards would need to focus on secure development, identity management, patching, and configuration management and would be made part of Federal Acquisition Regulations (FAR), making them part of the federal government's approach to buying and utilizing IoT. Thereafter, federal agencies and contractors would need to use and buy IoT that meets the new security standards.

There are a number of substantive changes from the initial bill. The revised bill would still apply to virtually all civilian government agencies, including independent agencies like the Securities and Exchange Commission (SEC). However, the initial bill would have included "national security systems," meaning most of the Department of Defense (DOD), the Intelligence Community (IC) agencies, but now those systems have been exempted. Also, the discretion provided to OMB under the bill introduced in March to revise or modify the definition of a covered device has been removed. Additionally, there is new language that would allow an "interested party" to petition OMB to remove a "covered device" from the requirements put in place under the bill.

Likewise, the bill is more directive in how the agencies must discharge their responsibilities. For example, under the initial bill, OMB was tasked with developing the guidelines on "the appropriate use and management by the agencies of covered devices owned or controlled by the agencies; and minimum information security requirements for managing security vulnerabilities associated with such devices." Under the revised bill, NIST must submit these guidelines to OMB, and then OMB and CISA will draft the standards that IoT owned or controlled by the federal government must meet, which will include those already in existence for much of the federal civilian government's information technology systems. These standards will then be added to the FAR. The bill also spells out with greater specificity the security vulnerability process guidelines the agencies will need to put in place. NIST will now submit guidelines to OMB, which will then develop standards that federal contractors must ultimately meet as a condition of their contracts with federal agencies. Again, these standards would be enshrined in the FAR.

**Further Reading**

"Proposed State Department bureau takes wrong approach to U.S. cyber diplomacy" – *cyberscoop*
"New Election Security Bills Face a One-Man Roadblock: Mitch McConnell" – *The New York Times*
"Russian disinformation on YouTube draws ads, lacks warning labels: researchers" – *Reuters*
"Huawei Tells Parliament It's No Security Threat, Aiming to Avoid a Ban" – *The New York Times*
"Battered Chinese companies put American plans on hold as trade war rattles confidence in US" – *South China Morning Post*
"LG Electronics, regulators oppose Qualcomm's effort to put antitrust ruling on hold" – *Reuters*

"Bolton Says U.S. Is Expanding Offensive Cyber Operations" – *The Wall Street Journal*
"U.S. Escalates Online Attacks on Russia's Power Grid" – *The New York Times*
"Huawei asks Verizon to pay over $1 billion for over 230 patents: source" – *Reuters*