Technology Policy Update
17 October 2019
By Michael Kans, Esq.

Spotlight: A Privacy Bill A Week

Last week, we took a look at Senate Finance Committee Ranking Member Ron Wyden (D-OR) released the "Consumer Data Protection Act" discussion draft, section-by-section, and one-pager, legislation not to be confused with Senator Bob Menendez's (D-NJ) "Consumer Data Protection Act" (S. 2188), a data security and breach notification bill.As discussed at some length, in short, Wyden's bill would vastly expand the power of the Federal Trade Commission (FTC) to police both the security and privacy practices off many U.S. and international multinational companies. The FTC would receive the authority to levy fines in the first instance, potentially as high as the European Union's General Data Protection Regulation of 4% of annual gross revenue. Moreover, the operative definition of the "personal information" that must be protected or subject to the privacy wishes of a consumer is very broad. The bill would also sweep into the FTC's jurisdiction artificial intelligence (AI) and algorithms (i.e. so-called big data).

While the "Consumer Privacy Protection Act of 2017" (H.R. 4081) from the 115th Congress also focuses on data security, it still contains provisions that would require those entities covered by the bill to better protect consumers' privacy. Representative David Cicilline (D-RI) sponsored the House bill and is now the chairman of the House Judiciary Committee's Antitrust, Commercial and Administrative Law Subcommittee that is conducting an investigating into possible anti-competitive practices in the technology industry. 11 other House Democrats cosponsored this bill, which was not considered at all in the last Congress. Senator Patrick Leahy (D-VT) and some Senate Democrats introduced S. 2124, a bill that is substantially similar to the House version.

Not surprisingly, this bill would make certain conduct related to data security subject to possible criminal liability. This would differentiate this bill from a number of the other bills, save for Senator Ron Wyden's (D-OR) discussion draft. A likely reason for this difference is that a number of the sponsors of both bills serve on the Judiciary Committees, and in order for data security and privacy bills to be referred to those committees there must be matter in the bill subject to the jurisdiction of those committees. However, this is not to suggest there is merely craven politics at work. Instead there is likely legitimate concern that the problems presented by these areas will not be solved absent stiff penalties for egregious conduct.

Generally, covered entities must design a consumer privacy and data security program tailored to the risks associated with the entity's data activities, including conducting risk assessments, managing and controlling risks, performing vulnerability tests, and periodically assessing and upgrading hardware, software, and technology. Covered entities would include almost all entities except those in compliance with the Financial Services Modernization Act of 1999 (aka Gramm-Leach-Bliley) or Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act and "service providers" (i.e. ISPs that are solely engaged in the "transmission, routing, or temporary, intermediate, or transient storage of [electronic] communication." An additional exception exists for those entities that would be otherwise covered, for there is a threshold of collecting, using, storing, transmitting or disposing at least 10,000 people in any 12-month period before the data security requirements of the bill attach.

"Sensitive personally identifiable information" is defined as "any information or compilation of information, in electronic or digital form that includes" the usual sort of information policymakers want protected (e.g. Social Security number, driver's license, biometric data, etc.) However, this definition sweeps into it the types of data protected under HIPAA/HITECH Act regulations, geolocation data, financial account numbers or credit or debit card numbers, and password-protected digital photographs and digital videos not otherwise available to the public.

The FTC is directed to promulgate regulations under APA notice and comment procedures, but the phrasing suggests the FTC's latitude in drafting regulations may be limited. The bill provides that covered entities must comply with "following safeguards and any other administrative, technical, or physical safeguards identified by the FTC in a rulemaking process…for the protection of sensitive personally identifiable information." Consequently, covered entities would need to understand and hew to the new consumer privacy and data security program laid out in Section 202(a) and the subsequent "other administrative, technical, or physical safeguards identified by the FTC" in a rulemaking, possibly leading to additional to be determined requirements. Additionally, the choice of the word "identified" is what seems to be key here. A fair reading of this provision is that the FTC would merely identify the additional standards as opposed to a traditional rulemaking under which the agency would have greater discretion to determine the standards with which entities should comply. Additionally, the bill stipulates covered entities must "implement a consumer privacy and data security program pursuant to this subtitle" within one year of enactment. However, there is no timeline by which the FTC must promulgate its regulations. So, covered entities would need to read the requirements in Subtitle A of Title II (i.e. Consumer Privacy and Security of Sensitive Personally Identifiable Information) and make their best effort to comply and then wait for the FTC's additional regulations at some point in the future.

With respect to enforcement, either the Department of Justice (DOJ) or the FTC could file civil litigation in federal court. Both agencies could seek fines of up to $16,500 per individual whose sensitive personally identifiable information has been breached with a cap of $5 million on total fines unless the conduct is found to be willful and intentional at which point fines would be uncapped. Like the other bills, the FTC may treat alleged violations of the new security and privacy regime as a "unfair or deceptive act or practice in commerce in violation of a regulation," allowing the agency to pursue civil fines in the first instance. State attorneys general could also bring actions under this section but usually only after alerting the DOJ and the FTC.

H.R. 4081 does not create a private right of action for consumers allegedly harmed by a breach but it explicitly does not preempt avenues a consumer could file a lawsuit under state laws (e.g. tort or contract actions). Likewise, the bill sets a floor for security and privacy standards and only those state laws less stringent than the new federal regime would be preempted.

As mentioned, some failures to meet the requirements of this bill would result in criminal liability. Title I of the bill would make it a felony to conceal a security breach of sensitive personally identifiable information. However, any such person accused of concealing such a breach must have knowledge of the breach, must "intentionally and willfully" act to conceal, and the breach must result in economic harm to at least one person in the amount of at least $1,000. This title would also require the Department of Justice (DOJ) to report on the number of prosecutions under the Computer, Fraud and Abuse Act (CFAA) related to exceeding authorization on a computer system or unauthorized access to a computer system. The federal government would also receive authority to shut down bot networks.

Second Volume of Senate Intelligence Committee Report On Election Interference

The Senate Intelligence Committee released the second of five planned volumes detailing its findings and recommendations arising from Russia's actions during the 2016 U.S. election. Notably, the Senate Intelligence Committee broke with the Intelligence Community's finding that Russian efforts were mostly aimed against former Secretary of State Hillary Clinton; rather the Committee found the Russian social media campaign "was overtly and almost invariably supportive of then-candidate Trump, and to the detriment of Secretary Clinton's campaign." The committee found that there was a dedicated campaign to suppress African American voting. Moreover, paid advertisements were the lesser part of Russian efforts. The committee has found that Russian hackers continue to post divisive, misleading, and false messages on social media to further foment unrest and division in the U.S.

The committee called on the tech industry to ramp up information sharing efforts, increase the information consumers are provided with regarding the source and veracity of social media posts, and allow researchers and presumably U.S. intelligence agencies greater access to the data held by companies like Twitter and Facebook to better track and counter the efforts of countries like Russia. In terms of legislative action, the committee recommended that Congress pass legislation to remove obstacles to the sharing of information between social media and government agencies, to create a clearinghouse of such information, and to continue to "examine the full panoply of issues surrounding social media, particularly those items that may have some impact on the ability of users to masquerade as others and provide inauthentic content…such as privacy rules, identity validation, transparency in how data is collected and used, and monitoring for inauthentic or malign content, among others, deserve continued examination." However, the committee did not call for the passage of privacy, data security, or election security legislation. The committee is recommending that the executive branch launch a public awareness initiative "focused on building media literacy from an early age would help build long-term resilience to foreign manipulation of our democracy," "stand up an interagency task force to continually monitor and assess foreign country's use of social media platforms for democratic interference," and "develop a clear plan for notifying candidates, parties, or others associated with elections when those individuals or groups have been the victim of a foreign country's use of social media platforms to interfere in an election."

Notably, the only dissenting views appended to the second volume are those of Senator Ron Wyden (D-OR), who placed the blame firmly on weak data security and privacy laws in the U.S. that allow social media platforms to be used to target certain slices of the populations:

> Broad, effective data security and privacy policies, implemented across the platforms and enforced by a tough, competent government regulator, are necessary to prevent the loss of consumers' data and the abuse of that data in election influence campaigns. Congress should pass legislation that addresses this concern in three respects. First, the Federal Trade. Commission must be given the power to set baseline data security and privacy rules for companies that store or share Americans' data, as well as the authority and resources to fine companies that violate those rules, Second; companies should be obligated to disclose how consumer information is collected and shared and provide consumers the names of every individual or institution with whom their data has been Third, consumers must be given the ability to easily opt out of commercial data sharing.

None of the committee Republicans disputed the report's findings or recommendations.

In "The Report of the Select Committee on Intelligence United States Senate On Russian Active Measures Campaigns And Interference In the 2016 U.S. Election: Volume 2: Russia's Use Of Social Media," the committee explained

> In 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency (IRA) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States.
> Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election.

The committee made a number of key findings, including:

- The Committee found, that the IRA sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Kremlin.
- The Committee found that the IRA's information warfare campaign was broad in scope and entailed objectives beyond the result of the 2016 presidential election. Further, the Committee's analysis of the IRA's activities on social media supports the key judgments of the January 6, 2017 Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent US Elections," that "Russia's, goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency." However, where the Intelligence Community assessed that the Russian government "aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him," the Committee found that IRA social media activity was overtly and almost invariably supportive of then-candidate Trump, and to the detriment of Secretary Clinton's campaign.
- The Committee found that the Russian government tasked and supported the IRA's interference in the 2016 U.S. election. This finding is consistent with the Committee's understanding of the relationship between IRA owner Yevgeniy Prigozhin and the Kremlin, the aim and scope of the interference by the IRA, and the correlation between the IRA's actions and electoral interference by the Russian government in other contexts and by other means. Despite Moscow's denials, the direction and financial involvement of Russian oligarch Yevgeniy Prigozhin, as well as his close ties to high-level Russian government officials including President Vladimir Putin, point to significant Kremlin support, authorization, and direction of the IRA's operations and goals.
- The Committee found that Russia's targeting of the 2016 U.S. presidential election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society. Moreover, the IRA conducted a vastly more complex and strategic assault on the United States than was initially understood. The IRA's actions in 2016 represent only the latest installment in an increasingly brazen interference by the Kremlin on the citizens and democratic institutions of the United States.
- Analysis of the behavior of the IRA-associated social media accounts makes dear that while the Russian information warfare campaign exploited the context of the election and election-related issues in 2016, the preponderance of the operational focus, as reflected repeatedly in content, account names, and audiences targeted, was on socially divisive issues-such as race, immigration, and Second Amendment rights-in an attempt to pit

Americans against one another and against their government. The Committee found that IRA influence operatives consistently used hot-button, societal divisions in the United States as fodder for the content they published through social media in order to stoke anger, provoke outrage and protest, push Americans further away from one another, and foment distrust in government institutions. The divisive 2016 U.S. presidential election was just an additional feature of a much more expansive, target-rich landscape of potential ideological and societal sensitivities.

- The Committee found that the IRA targeted not only Hillary Clinton, but also Republican candidates during the presidential primaries. For example, Senators Ted Cruz and Marco Rubio were targeted and denigrated, as was Jeb Bush. As Clint Watts, a former FBI Agent and expert in social media weaponization, testified to the Committee, "Russia's media outlets and covert trolls sought to sideline opponents on both sides of the geopolitical spectrum with adversarial views towards the Kremlin." IRA operators sought to impact primaries for both major parties and "may have helped sink the hopes of candidates more hostile to Russian interests long before the field narrowed."
- The Committee found that no single group of Americans was targeted by IRA information operatives more than African-Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016. Evidence of the IRA's overwhelming operational emphasis on race is' evident in the IRA's Facebook advertisement content (over 66 percent contained a term related to race) and targeting (locational targeting was principally aimed at African-Americans in key metropolitan areas with), its Facebook pages (one of the IRA's top-performing pages, "Blacktivist," generated 11.2 million engagements with Facebook users), its Instagram content (five of the top 10 Instagram accounts were focused on African-American issues and audiences), its Twitter content (heavily focused on hot-button issues with racial undertones, such as the NFL kneeling protests), and its YouTube activity (96 percent of the IRA's YouTube content was targeted at racial issues and police· brutality).
- The Committee found that paid advertisements were not key to the IRA's activity, and moreover, are not alone an accurate measure of the IRA's operational scope, scale, objectives, despite this aspect of social media being a focus of early press reporting and public awareness. An emphasis on the relatively small number of advertisements, and the cost of those advertisements, has detracted focus from the more prevalent use of original, free content via multiple social media platforms. According to Facebook, the IRA spent a total-of about $100,000 over two years on advertisements-a minor amount, given the operational costs of the IRA were approximately $1.25 million dollars a month. The nearly 3,400 Facebook and Instagram advertisements the IRA purchased are comparably minor in relation to the over 61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets that were the original creations of IRA influence operatives, disseminated under the guise of authentic user activity.
- The Committee found that the IRA coopted unwitting Americans to engage in offline activities in furtherance of their objectives. The IRA's online influence operations were not constrained to the unilateral dissemination of content in the virtual realm, and its operatives were not just focused on inciting anger and provoking division on the internet. Instead, the IRA also persuaded Americans to deepen their engagement with IRA operatives. For example, the IRA targeted African-Americans over social media and attempted and succeeded in some cases to influence their targets to sign petitions, share personal information, and teach self-defense training courses. In addition, posing as U.S. political activists, the IRA requested-and in some cases obtained-assistance from the Trump Campaign in procuring materials for rallies and in promoting and organizing the rallies.

- The Committee found that the IRA was not Russia's only vector for attempting to influence the United States through social media in 2016. Publicly available information showing additional influence operations emanating from Russia unrelated to IRA activity make clear the Kremlin was not reliant exclusively on the IRA in 2016. Russia's intelligence services, including the Main Directorate of the General Staff of the Armed Forces of the Russian (GRU), also exploited U.S. social media platforms as a vehicle for influence operations. Information acquired by the Committee from intelligence oversight, social media companies, the Special Counsel's investigative findings, and research by commercial cybersecurity companies all reflect the Russian government's use of the GRU to carry out another core vector of attack on the 2016 election: the dissemination of hacked materials.
- The Committee found that IRA activity on social media did not cease, but rather increased after Election Day 2016. The data reveal increases in IRA activity across multiple social media platforms, post-Election Day 2016: Instagram activity increased 238 percent, Facebook increased 59 percent, Twitter increased 52 percent, and YouTube citations went up by 84 percent. As John Kelly noted: "After election day, the Russian government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is. much bigger than the attack on a single election.'
- Though all of the known IRA-related accounts from the Committee's data set were suspended or taken down in the fall of2017, outside researchers continue to uncover additional IRA social media accounts dedicated to spreading malicious content. According to an October 2018 study of more than 6.6 million tweets linking to publishers of intentionally false news and conspiracy stories, in the months before the 2016 U.S. election, "more than 80% of the disinformation accounts in our election maps are still active ... [and] continue to publish more than a million tweets in a typical day."

The committee made a number of recommendations with this preface:

> This challenge requires an integrated approach that brings together the public and private sectors. This approach must be rooted in protecting democratic values, including freedom of speech and the right to privacy. The Federal government, civil society, and the private sector, including social media and technology companies, each have an important role to play in deterring and defending against foreign influence operations that target the United States.

A. Industry Measures

- The Committee recommends that social media companies work to facilitate greater information sharing between the public and private sector, and among the social companies themselves about malicious activity and platform vulnerabilities that are exploited to spread disinformation. Formalized mechanisms for collaboration that facilitate content sharing among the social media platforms in order to defend against foreign disinformation, as occurred with violent extremist content online, should be fostered. As researchers have concluded: "Many disinformation campaigns and cyber threats do not just manipulate one platform; the information moves across various platforms or a cyber-attack threatens multiple companies' network security and data integrity. There must be greater cooperation within the tech sector and between the tech sector and other stakeholders to address these issues." The Committee agrees.
- This should not be a difficult step. Models for cooperation already exist and can be developed further:

- Google, Facebook, Twitter, and Microsoft already maintain a common database of digital fingerprints identifying violent extremist videos. These four companies also participate in a Cyberhate Problem-Solving Lab run by the Anti-Defamation League's Center for Technology and Society.
- Dozens of tech companies participate in the Global Network Initiative, a tech policy forum devoted to protecting digital rights globally.
- Other examples include the Global Internet Forum to Counter Terrorism, whose goal is to substantially disrupt terrorists' ability to disseminate violent extremist propaganda, and glorify real-world acts of violence; and the National Cyber Forensics and Training Alliance, a nonprofit partnership between industry, government, and academia that enables cooperation to disrupt cyber-crime. ·
- Two models from the world of financial intelligence are the UK's Joint Money Laundering Intelligence Taskforce the United States' Financial Crimes Enforcement. Exchange.
- At the urging of the Committee, social media companies have begun to share indicators, albeit on an ad hoc basis.
- The Committee further recommends that social media companies provide users with:
  - Greater transparency about activity occurring on their platforms, including disclosure of automated accounts (i.e., bots);
  - Greater context for users about why they see certain content;
  - The locational origin of content; and,
  - Complete and timely public exposure of malign information operations.

- Social media platforms are not consistent in proactively, clearly, and conspicuously notifying users that they have been exposed to these efforts, leaving those who have been exposed to the false information or accounts without the knowledge they need to better evaluate future social media content that they encounter. Notifications to individual users should be clearly stated, device neutral, and provide users all the information necessary to understanding the malicious nature of the social media content or accounts they were exposed to.
- Finally, the analytic and computational capabilities of outside researchers should be put to greater use by the social media companies. Although social media companies have released some data about the manipulation of their platforms by foreign actors, the Committee recommends that social media companies be more open to facilitating third-party research designed to assist them in defending their platforms from disinformation campaigns. The results of collaboration with outside researchers should be shared with users who have been exposed to disinformation.

B. Congressional Measures

- The Committee recommends that Congress· consider ways to facilitate productive coordination and cooperation between U.S. social media companies and the pertinent government agencies and departments, with respect to curtailing foreign influence operations that target Americans-to include examining laws that may impede that coordination and cooperation. Information sharing between the social media companies and law enforcement must improve, and in both directions. Data must be shared more quickly and in a more useful manner. This will improve the ability of social media companies to quickly identify and disclose malign !foreign influence operations to the(appropriate authorities, and it will improve the ability of law enforcement agencies to respond in a timely manner.
- Informal channels of communication may not be sufficient to accomplish this goal. As part of its examination, Congress must assess whether formalized information sharing between law

enforcement and social media companies is useful and appropriate. Certain statutory models already exist, such as U.S. Code, Title 18, Section' 2258A (Reporting requirements of providers). That section requires social media companies to report any apparent violations of laws relating to child sexual exploitation to the National Center for Missing and Exploited Children (NCMEC). NCMEC is a private, non-profit entity that serves a statutorily authorized clearinghouse role: it receives the providers' reports, assesses the reports for criminality and threats to children, and refers them to the appropriate law enforcement authorities for action. Formalizing a relationship between social media companies and the government does present some legal considerations,300 but these should not be prohibitive.

- Further, the Committee recommends that Congress examine legislative approaches to ensuring Americans know the sources of online political advertisements. The Federal Election Campaign Act of 1971 requires political advertisements on television, radio and satellite to disclose the sponsor of the advertisement. The same requirements should apply online. This will also help to ensure that the IRA or any similarly situated actors cannot use paid advertisements for purposes of foreign interference.
- Finally, Congress should continue to examine the full panoply of issues surrounding social media, particularly those items that may have some impact on the ability of users to masquerade as others and provide inauthentic content. Issues such as privacy rules, identity validation, transparency in how data is collected and used, and monitoring for inauthentic or malign content, among others, deserve continued examination. In addition, Congress should monitor the extent to which social media companies provide users with information laid out in section A and, if necessary, take remedial steps.

C. Executive Branch Measures

- The Committee recommends that the Executive Branch should, in the run up to the 2020 election, reinforce with the public the danger of attempted foreign interference in the 2020 election.
- Addressing the challenge of disinformation in the long-term will ultimately need to be tackled by an informed and discerning population of citizens who are both alert to the threat and armed with the critical thinking skills necessary to protect against malicious influence. A public initiative-propelled by federal funding but led in large part by state and local education institutions-focused on building media literacy from an early age would help build long-term resilience to foreign manipulation of our democracy. Such an effort could benefit from the resources and knowledge of private sector technology companies.
- Additionally, and in concert with initiatives that heighten public awareness about disinformation, media organizations should establish guidelines for using social media accounts as sources, to guard against quoting falsified accounts or state-sponsored disinformation.
- The Committee further recommends that the Executive Branch stand up an interagency task force to continually monitor and assess foreign country's use of social media platforms for democratic interference. The task force should periodically advise the public and Congress on its findings and issue annual reports providing recommendations to key actors, including executive branch departments and agencies, industry, and civil society. The task force should also develop a deterrence framework to inform U.S. Government responses to foreign influence efforts using social media.
- The Committee further recommends that the Executive Branch develop a clear plan for notifying candidates, parties, or others associated with elections when those individuals or groups have been the victim of a foreign country's use of social media platforms to interfere in an election. The plan should provide standards for deciding who to notify and when, and

should clearly delineate which agencies are responsible for making the notifications and to whom.

D. Other Measures

- The Committee recommends that candidates, campaigns, surrogates from campaigns, and other public figures engaged in political discourse on social media be judicious in scrutinizing the sources of information that they choose to share or promote online. Such public figures, precisely because of the reach of their networks, are valuable targets for adversaries, and can quickly be co-opted into inadvertently promoting a foreign influence operation.
- Amplification of foreign content, intentional or otherwise, is celebrated by those like the IRA, who wish to enflame our differences in order to advance their own interests. The Committee recommends that all Americans, and particularly those with a public platform, take on the responsibility of doing due diligence in their use of social media, so as to not give greater reach to those who seek to do our country harm.
- The Committee recommends the implementation of a Public Service Announcement (PSA) campaign, potentially by the" social media industry or by government actors, that promotes informed social media behavior and raises awareness about various types of foreign influence and interference activity that is targeting American citizens, businesses, and institutions. Foreign influence campaigns that target social media users in the United States should receive similar attentiontothedangersofsmokingandtheenvironmentalrisksofpollution. Broader exposure of specific foreign government linkages to social media content and influence activities would handicap the effectiveness of information operations.

CCPA Regulations Issued and CCPA Amendments Signed

California Attorney General (AG) Xavier Becerra has released draft regulations as required by the "California Consumer Privacy Act" (CCPA) (AB 375) and related explanatory materials. Per the CCPA, the AG has until July 1, 2020 to finish the promulgation and adoption of the regulations required under the act. Given the timeline laid out in the materials, the fastest such regulations could be finalized would likely be in late January or early February, which is a very optimistic projection. Rather, it is more likely that final regulations are issued late spring such as June. And, beyond the obvious reasons why the issuance of final regulations matters, the CCPA bars the AG from enforcing the bill for "six months after the publication of the final regulations issued...or July 1, 2020, whichever is sooner." At this point, it appears the date upon which enforcement of the CCPA begins will be July 1, 2020, for final regulations would have to be issued in late December to move that date forward at all, and this seems unlikely given the early December public meetings and deadline for input on the regulations. As explained in Becerra's press release, "[c]omments may be submitted to the Office of the Attorney General on or before 5:00 P.M. Pacific time on December 6, 2019...[and] [a]ll comments received by the deadline will be posted on the Attorney General's Office website and are subject to disclosure under the Public Records Act."

In the "Notice of Proposed Rulemaking Action," the AG's Office explained the CCPA "requires the Attorney General to solicit broad public participation and adopt regulations to further the purposes of the CCPA, including, but not limited to, the following areas:

(1) Updating as needed additional categories of "personal information" in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional

categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business.
(3) Establishing any exceptions necessary to comply with state or federal law.
(4) Establishing rules and procedures to facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information and a business's compliance with a consumer's opt-out request, and the development and use of a recognizable and uniform opt-out logo or button to promote consumer awareness of the opportunity to opt out of the sale of personal information.
(5) Adjusting the monetary threshold for the annual gross revenue included in the definition of "business."
(6) Establishing rules, procedures, and any exceptions necessary to ensure that businesses provide the notices and information required by the CCPA in a manner that may be easily understood by the average consumer, accessible to consumers with disabilities, and available in the language primarily used to interact with the consumer.
(7) Establishing rules and guidelines regarding financial incentive offerings.
(8) Establishing rules and procedures to further the purposes of Sections 1798.110 [i.e. the section directing businesses that collect information to inform consumers which information is collected and sold upon request] and 1798.115 [i.e. the section directing businesses that sell information to inform consumers which information is collected and sold upon request]
(9) Establishing rules and procedures to facilitate a consumer's or the consumer's authorized agent's ability to obtain information, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business.
(10) Establishing rules and procedures to govern a business' determination that a request for information received by a consumer is a verifiable request, including situations where the consumer has a password-protected account with the business and when they do not.
Some quick observations about the voluminous materials released by the AG's Office. First, the AG did not expand the statutory definitions of "personal information" "unique identifiers" as he could have. Nonetheless, those two terms are defined fairly broadly under the statute. Second, the only exceptions provided for covered entities under federal and state law are for purposes of responding to a consumers right to know request in that such statutes or regulations may bar the provision of such information. For example, presumably a covered entity could not inform a consumer that a law enforcement agency has requested information under a warrant or subpoena.

The CCPA draft regulations also impose additional responsibilities on any "business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers." These businesses must

(1) Compile the following metrics for the previous calendar year:
a. The number of requests to know that the business received, complied with in whole or in part, and denied;
b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.
(3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

The regulations also define "Financial incentive," a term not defined in the CCPA. The regulations provide this will be "a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information."

Of course, the CCPA grants further authority to the AG to "adopt additional regulations as necessary to further the purposes of the CCPA" at his discretion. One such instance where this power was not utilized, likely in response to a request, was by declining to deem those firms in compliance with the General Data Protection Regulation (GDPR) in the form of a safe harbor.

In the "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations" appended to the Initial Statement Of Reasons (ISOR) that was prepared by Berkeley Economic Advising and Research (BEAR), it is claimed that

- the "preliminary estimate of direct compliance costs is estimated to be $467-$16,454 million over the next decade (2020-30), depending on the number of California businesses coming into compliance"
- "[W]e generate a back of the envelope cost of CCPA compliance, including both the statute's baseline costs and the incremental costs attributable to the regulations, using estimates from the TrustArc survey cited above. Assume that smaller firms (<20 employees) will incur $50,000 in initial costs (the median of the lowest cost category)2, medium-sized firms (20-100 employees) incur an initial cost of $100,000 (the maximum of the lowest cost category in the survey), medium/large firms (100-500 employees) incur an initial cost of $450,000, and firms with greater than 500 employees incur, on average an initial cost of $2 million. Also assume that 75% of all California businesses will be required to comply with the CCPA (see Section 2.1 for detailed estimates of the number of firms affected by firm size and industry). The total cost of initial compliance with the CCPA, which constitutes the vast majority of compliance efforts, is approximately $55 billion. This is equivalent to approximately 1.8% of California Gross State Product in 2018."
- "As a lower-bound estimate of the number of businesses that will be required to comply with CCPA, we use 2017 Survey of U.S. Businesses (SUSB) data from the U.S. Census Bureau. This data reports the number of firms by sector and number of employees for California. Because the data does not include data on business revenue, we assume that the average employee generates approximately $100,000 in annual revenue. Based on this assumption, firms with more than 250 employees will meet the $25 million CCPA threshold. Employee size categories in the SUSB data are reported for businesses with 100-499 employees and businesses with 500 or more employees. We assume that all businesses with 500+ employees will be subject to the CCPA and 37.5% of businesses in the 100-499 employee category will need to comply with the law."
- "However, it is likely that the 50,000 PI requirement and the 50% annual revenue requirement will apply to many businesses with annual revenues less than $25 million. For example, any firm that collects personal information from more than 137 consumers or devices a day will meet the 50,000 threshold. To provide an upper bound on the number of firms potentially affected by the CCPA regulations, we consider two alternative

assumptions. We assume that either 50% or 75% of all California businesses that earn less than $25 million in revenue will be covered under than CCPA."

The AG's Office will hold four events on these draft regulations in early December:

- SACRAMENTO, Dec. 2, 2019, 10 a.m., CalEPA Building, Coastal Room 2nd Floor, 1001 I St., Sacramento, CA 95814
- LOS ANGELES, Dec. 3, 2019, 10 a.m., Ronald Reagan Building, Auditorium 1st Floor, 300 S. Spring St., Los Angeles, CA 90013
- SAN FRANCISCO, Dec. 4, 2019, 10 a.m., Milton Marks Conference Center, Lower Level, 455 Golden Gate Ave., San Francisco, CA 94102
- FRESNO, Dec. 5, 2019, 10 a.m., Hugh Burns Building, Assembly Room #1036, 2550 Mariposa Mall, Fresno, CA 93721

The AG's Office laid out next steps:

- After holding seven statewide public forums and reviewing over 300 written comments during the preliminary rulemaking stage, the Attorney General released draft regulations on October 10, 2019.
- The Attorney General will consider all comments and may revise the regulations in response.
- Any revision to the proposed regulations will be subject to an additional 15 day public comment period.
- Following the comment period, the Attorney General will submit the final text of the regulations, the final Statement of Reasons responding to every comment submitted, and an updated informative digest to the Office of Administrative Law (OAL). OAL has 30 working days to review the regulations, and if approved, the rules will go into effect.

Finally, on October 11, Governor Gavin Newsom signed the CCPA amendments the legislature sent him last month:

- A.B. 25 would exempt employers from the CCPA for only one year for activities related to collecting information from job applicants and employees.
    - A final legislature bill analysis posited "This bill reflects broad consensus reached by the author with stakeholders on an issue surrounding how to properly ensure that the CCPA applies to California consumers in the broadest of terms, without hindering the ability of businesses to appropriately collect PI from job applicants, employees, and similarly situated individuals, within employment-related contexts.
    - Specifically, as amended, this bill provides businesses a limited exemption from the CCPA until January 1, 2021, for PI that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's PI is collected and used by the business solely within the context of the natural person acting in one of those roles.
    - The Senate amendments also expressly specify that a business is exempt from the CCPA when: 1) collecting PI that is emergency contact information of such individuals, to the extent that the PI is collected and used solely within that context; and, 2) when PI is necessary to be retained for the administration of benefits to the extent that the PI is collected and used solely within the context of administering those benefits. Lastly, as amended, the bill includes two exceptions to the exemptions in order to ensure that the CCPA sections establishing a right to know what PI is being collected and to bring a limited private right of action for data breaches still apply.

- Ultimately, the one-year sunset provides the Legislature time to more broadly consider what privacy protections should apply in these particular employment-based contexts, and whether to repeal, revise, and/or make these exemptions permanent in whole or in part moving forward.

- A.B. 1564 would revise a requirement in the CCPA for businesses to make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA.
  - As introduced, this bill would have removed the toll-free number requirement in favor of an email address only and was later amended in the Assembly policy committee to require a physical address in addition to an email address unless the business operated exclusively online. This recognized that replacing a phone number with an email address would be insufficient to protect consumers who may not have access to the internet or who interact with a business only in their brick and mortar establishments due to lack of access issues. That being said, a concern remained relating to whether a physical address would be sufficient for timely access for such consumers.
  - As amended in the Senate, the bill instead reinstates the existing law toll free number requirement to ensure that such consumers have a readily accessible means of executing their CCPA requests and provides a limited exemption for businesses that operate exclusively online (to provide only an email address) consistent with the policy approved in the Assembly previously.
- A.B. 1146 would "narrowly limit[] the CCPA's opt-out and deletion rights in order to facilitate prompt and effective recalls and warranty work" of automobiles.
- A.B. 1355 "[a]ddresses various drafting errors and makes other clarifying changes in the California Consumer Privacy Act of 2018 (CCPA). Among other things, this bill also includes various provisions to clarify the scope and application of the CCPA's Fair Credit Report Act (FCRA) exemption; clarify obligations of businesses around collecting and retaining PI it would not otherwise collect or retain in the ordinary course of business; and address the application of the CCPA to business- to-business communications and transactions, as specified."
  - The Senate amendments would:
    - 1) Revise the existing FCRA exemption under the CCPA, as specified, and limit its application to exclude the CCPA's section establishing a data breach private right of action (PRA).
    - 2) Further clarify an existing CCPA exemption to specify that businesses do not need to collect PI that they would not otherwise collect in the ordinary course of their business or retain Personal Information (PI) for longer than they would otherwise retain in the ordinary course of their business.
    - 3) Specify that, until January 1, 2021, certain CCPA obligations do not apply to PI reflecting a communication or transaction between the business and the consumer, where the consumer is a natural person: 1) who is an employee, owner, director, officer, or contractor of a government agency or a business, as specified; and, 2) whose communications or
    - transactions with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from that business or government agency (i.e., "business-to-business" communications or transactions).
    - 4) Add express authority for the Attorney General (AG) to establish additional rules and procedures on how to process and comply with

verifiable consumer requests for specific pieces of PI relating to a household, as specified.
        - 5) Revise the CCPA section establishing a data breach PRA to clarify it applies to any consumer whose "nonencrypted and nonredacted" PI is subject to an unauthorized access and exfiltration, theft, or disclosure, as specified.
- A.B. 874 would expand the definition of "publicly available" information that is exempted from the definition of "personal information" (PI) in the CCPA to ensure that "publicly available" information includes any information that is lawfully made available from government records.
    - The CCPA specifically excludes certain information from the definition of personal information:
        - "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.
        - This bill amends this paragraph in several ways. First, it removes the phrase "if any conditions associated with such information." This language is a clear drafting error, as the clause does not make sense. The Assembly Privacy and Consumer Protection Committee analysis of this bill makes clear that the original language intended here was "where any conditions associated with such information are followed." This clause would provide some constraint on what is considered publicly available compared to simply removing the language currently in statute.
        - Second, this bill clarifies that personal information, rather than publicly available information, does not include deidentified or aggregate information. This was likely the intent of the language. This change simply clarifies that when information is deidentified or aggregated it is not considered personal information and is therefore not covered by the protections and protocols laid out in the CCPA. As "deidentified" and "aggregated consumer information" are currently defined, such information is not able to be associated back to an individual and certain protective measures are required, such as the implementation of business processes to prevent the accidental release of such information. Therefore, excluding such information from the protections of the CCPA is of little consequence.
- A.B. 1202 "[r]equires, on or before January 31 following each year in which a business meets the definition of data broker, that the business shall register with the Attorney General, as provided.
    - Requires data brokers to pay a registration fee in an amount determined by the Attorney General, not to exceed the reasonable costs of establishing and maintaining the informational Internet Web site that this bill requires the Attorney General to create and make accessible to the public.

- Requires data brokers to provide, and the Attorney General to include on its Web site, the name of the data broker and its primary physical, email, and Internet Web site addresses. Data brokers may, at their discretion, also provide additional information concerning their data collection practices.
- Subjects a data broker that fails to register as required by this section to injunction and civil penalties, fees, and costs to be recovered in an action brought in the name of the people of the State of California by the Attorney General. The remedies include civil penalties of $100 for each day the data broker fails to register; a monetary award in an amount equal to the fees that were due during the period it failed to register; and expenses incurred by the Attorney General in the investigation and prosecution of the action as the court deems appropriate.
- Provides that any penalties, fees, and expenses recovered in such actions are to be deposited in the Consumer Privacy Fund, to be used to fully offset the relevant costs incurred by the state courts and the Attorney General.
- Defines "data broker" as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The definitions specifically excludes the following:
    - a) a consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
    - b) a financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations; and
    - c) an entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Ins. Code § 1791 et seq.).

Finally, the Governor signed another bill that does not explicitly pertain to the CCPA, but it revises the definition of "personal information" that is operative for purposes of when a consumer may use an entity for violations of the CCPA:

- A.B. 1130
    - Expands this definition of personal information in the data breach notification statutes and Section 1798.81.5 to include an individual's first name or first initial and last name in combination with any of the following data elements, when either the name or the data elements are not encrypted (or redacted):
        - tax identification number;
        - passport number;
        - military identification number;
        - other unique identification number issued on a government document
        - commonly used to verify the identity of a specific individual; or
        - unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual, but not including a physical or digital photograph, unless used or stored for facial recognition purposes.
    - Provides that, in breaches involving biometric data, a person or business required to send a breach notification to a resident may include instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

In all likelihood, these will be the last changes made to the CCPA via legislation before the new statute takes effect on January 1, 2020 and is enforced starting no later than July 1, 2020. Now, the focus on the CCPA will turn to the draft regulations released for comment and the ballot initiative

to get "The California Privacy Rights and Enforcement Act of 2020" (CPREA) enacted (aka CCPA 2.0).

McAleenan Resigns

Last week, acting Secretary of Homeland Security Kevin McAleenan stepped down, but the Trump Administration did not name an appointee to permanently fill the role. Transportation Security Administration head David Pekoske was named acting Secretary, making him the fifth person to fill the role in the three years of the Trump Administration. In contrast, President Barack Obama had two Secretaries during his eight-year term. At this point, it is not clear how churn at the top of the department may be affecting cybersecurity policy given the relative stability in the leadership of the Department of Homeland Security's (DHS) cybersecurity components. However, these elements may be at a disadvantage relative to the Departments of Defense or Justice when it comes to inter-agency jockeying on certain policy initiatives or in visibility at the White House.

McAleenan was named the acting Secretary after the last Senate-confirmed Secretary, Kirstjen Nielsen, stepped down in April over allegations leveled by President Donald Trump during Cabinet meetings that she had failed to secure the U.S.-Mexico border. Other reports indicate Nielsen disagreed with and would oppose implementing a policy whereby the children of undocumented entrants to the U.S. would be separated from their parents.

The former National Protection and Programs Directorate (NPPD) and Cybersecurity and Infrastructure Security Agency (CISA) have been led by Christopher Krebs since 2017, and he was later confirmed as the head of NPPD in 2018. Assistant Director for Cybersecurity Jeanette Manfra has been in her current role since 2017, and before that she served as a senior advisor to former Secretary Jeh Johnson.

CISA Asks Congress For Subpoena Authority

While nothing official has been released, there are reports that the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is requesting that Congress grant the agency authority to administratively subpoena the identity of operators of critical but vulnerable cyber infrastructure from internet service providers (ISP). The agency allegedly has the operators of industrial systems in mind. Notably, administrative subpoenas can be issued by a number of law enforcement agencies without assent from a court. DHS officials have claimed the power would be used sparingly and only to make the owners and operators of some at risk critical infrastructure "more motivated." Reportedly the request has been made to the House and Senate Homeland Security Committees, but legislation has not been released by either the Trump Administration or Congress.

At present, ISPs cannot turn over the identity of its customers to a government agency absent a subpoena or a warrant, and law enforcement agencies can typically only issue administrative subpoenas as part of an investigation. Consequently, CISA, which lacks this authority, can seek and obtain the ownership of critical infrastructure that is at risk by piggybacking on a sister agency's authority. CISA is asking for its own standalone authority to clear up these problems. CISA's Assistant Director for Cybersecurity and Communications Jeannette Manfra told reporters '[a] challenge that we have is that we can see a lot of industrial control systems…that have potential vulnerabilities that are accessible from the public internet." Supposedly, CISA can only ask the ISP to pass along its concerns or intelligence to targeted owners or operators. Speaking publicly, CISA Director

Christopher Krebs remarked that "[w]hat we want to be able to do is if we can't resolve the issue through any other way, then we should be able to go to an ISP and say, 'We're concerned about this, can you provide us your customer contact information so we can go let them know that they have whatever port open or are running a vulnerable system."

When asked if DHS might not read and use its authority as expansively as possible as many agencies do, Manfra claimed "[w]e have a long history of collecting similar types of data through voluntary programs and [have] demonstrated ways of protecting that, as well as to ensure that the information is only used for the purposes that it was collected." She contended that CISA would use this authority in "very narrow set of circumstances." Representatives of the Homeland Security committees acknowledged receiving such a request from CISA, but their remarks diverged on how receptive lawmakers and staff were. A Senate Homeland Security staffer claimed the committee is looking at legislative solutions while a House Homeland Security aide expressed interest in ensuring CISA has the authority it need so long as proper privacy protections are put in place.

FISC Finds FBI Failed To Follow FISA and Fourth Amendment

This month an October 2018 U.S. Foreign Intelligence Surveillance Court (FISC) ruling was unsealed that held the Federal Bureau of Investigation's (FBI) use of Section 702 of the PATRIOT Act, which allows "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." While the ruling was heavily redacted, it was clear that the FBI was not following the statutory and Constitutional limits on its ability to query the surveillance obtained under Section 702. In particular, FISC found that "that the FBI Querying Procedures do not comply with the recordkeeping requirement at § 702(f)(l)(B) and that, in view of the FBI's querying practices, the FBI Querying Procedures and FBI Minimization Procedures do not, as implemented, satisfies the definition of "minimization procedures" at 50 U.S.C. § 1801(h) and are unreasonable under the Fourth Amendment."

Section 702 was last reauthorized in 2018 as part of the "FISA Amendments Reauthorization Act of 2017" (P.L. 115-118). This provision has been the statutory basis for the PRISM program exposed by former National Security Agency (NSA) contractor Edward Snowden under which the Intelligence Community acquires information from companies like Google and Yahoo. And, during the reauthorization there was concern that Section 702 served as a backdoor for the U.S. government to surveil Americans as opposed to other provisions of the Foreign Intelligence Surveillance Act that have more stringent requirements. Senator Mike Lee (R-UT) asserted that

> FISA 702 opened a backdoor to government spying on American citizens. This incidental spying is a different matter al-together, and it does implicate the Fourth Amendment—certainly the spirit of the Fourth Amendment if not also the letter thereof. It is profoundly worrying that the government maintains vast collections of information about American citizens, no matter how that information is collected, incidentally or intentionally. It is likewise worrying that the government cannot or will not say, specify, list exactly how many Americans have been subjected to government snooping under this provision.

However, a majority of both houses disagreed with this position. Senator Dianne Feinstein (D-CA) stated that

> U.S. persons cannot be targeted under section 702, but they can be collected incidentally if the individual is communicating with a non-U.S. person who is located overseas and is

> targeted under section 702. If an American's communications are collected incidentally, they are added to the 702 data-base. The government can later search, or query, that database for any American and gain access to the contents of any phone calls or emails that may have been swept up in the section 702 collection. Each of these queries results in the government's accessing the contents of a U.S. person's communications without ever going before a judge or securing a warrant. The Fourth Amendment requires the government to obtain a warrant based on probable cause before accessing those communications, and the Supreme Court has been clear: Americans have a right to privacy in the content of their phone calls and emails. The same standard should apply to communications incidentally collected under section 702.

FISC explained that

> Section 702(d)(l) requires targeting procedures to be "reasonably designed" to "ensure that any acquisition authorized under[§ 702(a)] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Additionally, the government uses the targeting procedures to ensure acquisitions do "not intentionally target a United States person reasonably believed to be located outside the United States." § 702(b)(3). Pursuant to § 702(i)(2)(B), the Court assesses whether the targeting procedures satisfy those criteria. The Court must also assess whether the targeting procedures, along with the querying and minimization procedures, are consistent with the requirements of the Fourth Amendment.

FISC stated that "[a]fter reviewing the applicable statutory provisions…the Court finds that the FBI's querying procedures do not comply with the requirement at Section 702(t)(l)(B) to keep records of U.S.-person query terms used to conduct queries of information acquired under Section 702." The court stated that "[i]t ultimately finds the FBI's querying and minimization procedures, as implemented, to be inconsistent with statutory minimization requirements and the requirements of the Fourth Amendment."

FISC noted that "[s]ince April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of crime." The court claimed that "[i]n a number of cases, a single improper decision or assessment resulted in the use of query terms corresponding to a large number of individuals, including U.S. persons." The FISC stated that "[t]he government acknowledges that such queries generally resulted from "fundamental misunderstandings by some FBI personnel [about] what the standard 'reasonably likely to return foreign intelligence information' means."

The FISC stated that "queries that lack a sufficient basis are not reasonably related to foreign intelligence needs and any resulting intrusion on U.S. persons' privacy lacks any justification recognizedby§1801(h)(l)." The FISC said that "[b]ecause the FBI procedures, as implemented, have involved a large number of unjustified queries conducted to retrieve information about U.S. persons, they are not reasonably designed, in light of the purpose and technique of Section 702 acquisitions, to minimize the retention and prohibit the dissemination of private U.S. person information."

The FISC stated that

> Those instances of non-compliant queries, in the Court's view, do not present the same level of concern as those that evidence misunderstanding of the querying standard. It would be difficult to completely prevent personnel from querying data for personal reasons. As a general rule, inadvertent queries of Section 702 information and queries intended to retrieve finished intelligence reports or other FBI work product do not seem likely to return raw 702 information or, if they happen to do so, to result in personnel examining U.S.-person information contained therein, the above-described queries regarding notwithstanding.

The FISC stated that "[o]f serious concern, however, is the large number of queries evidencing misunderstanding of the querying standard -- or indifference toward it: queries were conducted against the advice of FBI Office of General Counsel (OGC)." The court stated that "[t]hat concern is heightened by three factors: (1) limitations on the government's oversight mechanisms; (2) the FBI's policy to encourage routine and maximal querying of Section 702 information; and (3) apparent complications in applying the querying standard." The FISC determined that "[g]iven the limitations on the oversight of FBI querying practices, it appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the Court."

However, FISC noted that "[i]n other respects, the government's querying and minimization procedures…comport with applicable statutory requirements and the Fourth Amendment." The court added that "[i]n particular, the changes to the FBI Minimization Procedures that provide more detailed guidance on the storage and handling of information on various types of systems and related organizational changes to those procedures, see March 27, 2018, Memorandum at 43-70, 74-75, present no impediment to making those findings."

OECD Releases International Digital Tax Framework

Last week, the Organisation for Economic Co-operation and Development (OECD) Secretariat "published a proposal to advance international negotiations to ensure large and highly profitable Multinational Enterprises, including digital companies, pay tax wherever they have significant consumer-facing activities and generate their profits" according to the OECD press release. This proposal could form the basis for an international revamp of how companies, particularly technology companies, are taxed going forward.

Taxation of digital companies has been a recent focus in Europe. In 2016 EU Competition Commissioner Margrethe Vestager determined that Apple should pay €13 billion to atone for taxes the company illegally avoided in paying EU nations. Apple is appealing the determination. Earlier this year, the European Union's Council was blocked from acting on digital taxation by four countries: Denmark, Sweden, Finland, and Ireland, each of whom favored the current taxation scheme for different reasons. Reportedly Paris was pushing for a digital tax on companies like Google and Facebook, and subsequently the France enacted a 3% tax for companies with more than € 750 million (about $830 million) that has since been held in abeyance after U.S. protests

The OECD claimed that the proposal "brings together common elements of three competing proposals from member countries, and is based on the work of the OECD/G20 Inclusive Framework on BEPS, which groups 134 countries and jurisdictions on an equal footing, for multilateral negotiation of international tax rules, making them fit for purpose for the global economy of the 21st Century."

In the proposal, the OECD stated that "[t]he tax challenges of the digitalisation of the economy were identified as one of the main areas of focus of the Base Erosion and Profit Shifting (BEPS) Action Plan, leading to the 2015 BEPS Action 1 Report."

The OECD stated

> The proposal, which is now open to a public consultation process, would re-allocate some profits and corresponding taxing rights to countries and jurisdictions where MNEs have their markets. It would ensure that MNEs conducting significant business in places where they do not have a physical presence, be taxed in such jurisdictions, through the creation of new rules stating (1) where tax should be paid ("nexus" rules) and (2) on what portion of profits they should be taxed ("profit allocation" rules).

The OECD explained that "[t]he three alternatives set out in the Programme of Work under Pillar One have a number of significant commonalities:

- though there is some variation in how the proposals address the digitalisation issue, to the extent that highly digitalised businesses are able to operate remotely, and/or are highly profitable, all proposals would reallocate taxing rights in favour of the user/market jurisdiction;
- all the proposals envisage a new nexus rule that would not depend on physical presence in the user/market jurisdiction;
- they all go beyond the arm's length principle and depart from the separate entity principle; and
- they all search for simplicity, stabilisation of the tax system, and increased tax certainty in implementation

The OECD stated that

> That proposal is summarised here at a relatively general level, recognising that certain aspects still require further work. A number of implementation and administration questions also need to be addressed. However, the technical work of the Secretariat, as well as consultations with the membership, indicate that this is a viable option. It draws on the three alternatives under Pillar One and the ensuing public consultation process, and aims to identify the key features of a solution, which would include the following:
>
> - Scope. The approach covers highly digital business models but goes wider – broadly focusing on consumer-facing businesses with further work to be carried out on scope and carve-outs. Extractive industries are assumed to be out of the scope.
> - New Nexus. For businesses within the scope, it creates a new nexus, not dependent on physical presence but largely based on sales. The new nexus could have thresholds including country specific sales thresholds calibrated to ensure that jurisdictions with smaller economies can also benefit. It would be designed as a new self-standing treaty provision.
> - New Profit Allocation Rule going beyond the Arm's Length Principle. It creates a new profit allocation rule applicable to taxpayers within the scope, and irrespective of whether they have an in-country marketing or distribution presence (permanent establishment or separate subsidiary) or sell via unrelated distributors. At the same time, the approach largely retains the current transfer pricing rules based on the arm's length

principle but complements them with formula based solutions in areas where tensions in the current system are the highest.

- Increased Tax Certainty delivered via a Three Tier Mechanism. The approach increases tax certainty for taxpayers and tax administrations and consists of a three tier profit allocation mechanism, as follows:
    - –Amount A – a share of deemed residual profit6 allocated to market jurisdictions using a formulaic approach, i.e. the new taxing right;
    - –Amount B – a fixed remuneration for baseline marketing and distribution functions that take place in the market jurisdiction; and
    - –Amount C – binding and effective dispute prevention and resolution mechanisms relating to all elements of the proposal, including any additional profit where in-country functions exceed the baseline activity compensated under Amount B.

The OECD added:

> In a digital age, the allocation of taxing rights can no longer be exclusively circumscribed by reference to physical presence. The current rules dating back to the 1920s are no longer sufficient to ensure a fair allocation of taxing rights in an increasingly globalised world. It is also true that a number of the proposals that have already been made to address highly digitalised businesses fail to capture significant parts of the digitalised economy (such as digital services and certain high-tech businesses). The Secretariat's proposal is designed to respond to these challenges by creating a new taxing right.
> The Secretariat's proposal is designed to address the tax challenges of the digitalisation of the economy and to grant new taxing rights to the countries where users of highly digitalised business models are located. However, the approach also recognises that the transfer pricing and profit allocation issues at stake are of broader relevance.
> Against that background, the proposed "Unified Approach" would retain the current rules based on the arm's length principle in cases where they are widely regarded as working as intended, but would introduce formula-based solutions in situations where tensions have increased – notably because of the digitalisation of the economy.

US-Japan Trade Agreement Revamps Digital Commerce

Last week, U.S. Trade Representative (USTR) Robert Lighthizer and Ambassador of Japan to the United States Shinsuke J. Sugiyama signed two trade agreements, one of which, the "U.S.-Japan Digital Trade Agreement" is being billed as a revamp and improvement of the current arrangement, with other agreements to follow covering other sectors of U.S.-Japan trade. The USTR is also claiming these provisions are substantially similar to those in the North America Free Trade Agreement revisions (aka the United States-Mexico-Canada Agreement (USMCA)).

While the U.S. Senate will not have a chance to ratify the digital trade agreement because it is an executive agreement, Japan's Diet will need to ratify the agreement before it takes effect. However, some critics have claimed that the deal is illegal under the agreements that created the World Trade Organization (WTO) as Article XXIV of the General Agreement on Tariffs and Trade (GATT) requires such free trade agreements (FTA) to cover "substantially all trade," and these two agreements are piecemeal.

Moreover, this agreement comes a few years after the U.S. withdrew from the Trans-Pacific Partnership (TPP), a comprehensive trade agreement that excluded China, that was a key piece of the Obama Administration's pivot to the Pacific. The TPP was ultimately replaced by the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) after the Trump Administration withdrew from TPP negotiations.

According to an Obama Administration fact sheet:

> TPP will help preserve the open Internet and prevent its breakup into multiple, balkanized networks in which data flows are more expensive and more frequently blocked. The Electronic Commerce chapter will ensure the free flow of data (subject to public-interest regulation, for example to prevent spam, protect privacy, and fight cyber-crime); prevent the spread of 'forced localization' of technologies and servers; and help to more effectively guarantee the security and privacy of internet users. All this will help to unlock the promise of digital trade through rules that keep the Internet free and open, set digital trade rules-of-the-road, and provide the incentives and a stable framework that can nurture a healthy environment for companies and individuals as they create and use content.

According to a USTR fact sheet, "[a]s two of the most digitally-advanced countries in the world, the United States and Japan share a deep common interest in establishing enforceable rules that will support digitally-enabled suppliers from every sector of their economies to innovate and prosper, and in setting standards for other economies to emulate." The USTR contended that "[t]he United States-Japan Digital Trade Agreement parallels the United States-Mexico-Canada Agreement (USMCA) as the most comprehensive and high-standard trade agreement addressing digital trade barriers ever negotiated." The USTR stated that "[t]his agreement will help drive economic prosperity, promote fairer and more balanced trade, and help ensure that shared rules support businesses in key sectors where both countries lead the world in innovation." The USTR claimed that "[k]ey outcomes of this agreement include rules that achieve the following:

- Prohibiting application of customs duties to digital products distributed electronically, such as e-books, videos, music, software, and games.
- Ensuring non-discriminatory treatment of digital products, including coverage of tax measures.
- Ensuring that data can be transferred across borders, by all suppliers, including financial service suppliers.
- Facilitating digital transactions by permitting the use of electronic authentication and electronic signatures, while protecting consumers' and businesses' confidential information and guaranteeing that enforceable consumer protections are applied to the digital marketplace.
- Prohibiting data localization measures that restrict where data can be stored and processed, enhancing and protecting the global digital ecosystem; and extending these rules to financial service suppliers, in circumstances where a financial regulator has the access to data needed to fulfill its regulatory and supervisory mandate.
- Promoting government-to-government collaboration and supplier adherence to common principles in addressing cybersecurity challenges.
- Protecting against forced disclosure of proprietary computer source code and algorithms.
- Promoting open access to government-generated public data.
- Recognizing rules on civil liability with respect to third-party content for Internet platforms that depend on interaction with users.

- Guaranteeing enforceable consumer protections, including for privacy and unsolicited communication, that apply to the digital marketplace, and promoting the interoperability of enforcement regimes, such as the APEC Cross-Border Privacy Rules system (CBPR).
- Ensuring companies' effective use of encryption technologies and protecting innovation for commercial products that use cryptography, consistent with applicable law.

The USTR stated that "[t]ogether, these provisions will set predictable rules of the road and encourage a robust market in digital trade between the two countries – developments that should support increased prosperity and well-paying jobs in the United States and Japan."

EU Releases Plan To Coordinate 5G Risk Assessments

The European Union (EU) member states released "a report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks…[a] major step is part of the implementation of the European Commission Recommendation adopted in March 2019 to ensure a high level of cybersecurity of 5G networks across the EU" according to the EU's press release. These nations explained that the "report is based on the results of the national cybersecurity risk assessments by all EU Member States…[and] identifies the main threats and threats actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) and a number of strategic risks."

While not naming Huawei, the EU laid out considerations for each nation in building out its 5G network that seemed almost certainly aimed at the Chinese tech giant. Of course, even 5G networks built by Deutsche Telekom, Ericsson and Nokia must rely on the global supply chain, much of which originates or passes through China, posing many of the same risks Huawei would. Aside and apart from U.S. pressure on its allies and other nations not to use Huawei, recent reports that Huawei helped African regimes spy on dissidents stirred further concerns. Moreover, a 2017 Chinese law requiring its technology companies to cooperate with its intelligence efforts has given further pause to many nations.

The EU stated "the roll-out of 5G networks is expected to have the following effects:

- An **increased exposure to attacks and more potential entry points for attackers**: With 5G networks increasingly based on software, risks related to major security flaws, such as those deriving from poor software development processes within suppliers are gaining in importance. They could also make it easier for threat actors to maliciously insert backdoors into products and make them harder to detect.
- Due to new characteristics of the 5G network architecture and new functionalities, **certain pieces of network equipment or functions are becoming more sensitive**, such as base stations or key technical management functions of the networks.
- An increased exposure to risks related to the **reliance of mobile network operators on suppliers**. This will also lead to a higher **number of attacks paths that might be exploited by threat actors** and increase the potential severity of the impact of such attacks. Among the various potential actors, non-EU States or State-backed are considered as the most serious ones and the most likely to target 5G networks.
- In this context of increased exposure to attacks facilitated by suppliers, the **risk profile of individual suppliers** will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country.
- **Increased risks from major dependencies on suppliers**: a major dependency on a single supplier increases the exposure to a potential supply interruption, resulting for instance

from a commercial failure, and its consequences. It also aggravates the potential impact of weaknesses or vulnerabilities, and of their possible exploitation by threat actors, in particular where the dependency concerns a supplier presenting a high degree of risk.

- **Threats to availability and integrity of networks will become major security concerns**: in addition to confidentiality and privacy threats, with 5G networks expected to become the backbone of many critical IT applications, the integrity and availability of those networks will become major national security concerns and a major security challenge from an EU perspective.

The EU explained "[o]n 26 March 2019, after receiving the support from the European Council, the Commission adopted a Recommendation on Cybersecurity of 5G networks calling on Member States to complete national risk assessments and review national measures and to work together at EU level on a coordinated risk assessment and a common toolbox of mitigating measures." The EU laid out next steps:

- To complement the Member States' report, the European Agency for Cybersecurity is finalising a specific threat landscape mapping related to 5G networks, which considers in more detail certain technical aspects covered in the report.
- By 31 December 2019, the Cooperation Group should agree on a toolbox of mitigating measures to address the identified cybersecurity risks at national and Union level.
- By 1 October 2020, Member States – in cooperation with the Commission – should assess the effects of the Recommendation in order to determine whether there is a need for further action. This assessment should take into account the outcome of the coordinated European risk assessment and of the effectiveness of the measures.

Letter to OMB on ICT Supply Chain

The leadership of the Senate Homeland Security Committee and two other Senators sent a letter to the Director of the Office of Management and Budget (OMB) requesting that the Federal Acquisition Security Council (FASC) "develop a strategic plan for sharing supply chain security information with Congress and the judiciary to better protect U.S. government systems and enhance our national security." They noted that the two other branches of the federal government face the same cyber and supply chain threats facing the executive branch, and they urged OMB, which leads the FASC, to include Congress and the federal court system in its plans to share information regarding information and communications technology (ICT) supply chain risk management (SCRM) threats. The letter was signed by Senate Homeland Security Chair Ron Johnson (R-WI) and Ranking Member Gary Peters (D-MI) and Senators Ron Wyden (D-OR) and Tom Cotton (R-AR).

The Senators noted that "[a]s the Intelligence Community (IC) analyzes the information and communications technology (ICT) supply chain risk management (SCRM) threats and shares that information, through the FASC, with civilian agencies making security and acquisition decisions, it is important that this information also be provided to the other two branches of government." They argued that "[n]either Congress nor the judiciary has the resources, expertise, or mission to replicate the IC's SCRM work, meaning that the comprehensive "whole of government" approach the FASC was intended to achieve will likely only benefit one branch of the federal government...[which] leaves Congress and the courts at risk of introducing insecure ICT that is vulnerable to the national security threats assessed by the IC and FASC."

The Senators argued that the risks to the other two branches of government are very real:

- For the past three years, the U.S. Courts Information Systems and Cybersecurity Annual Report has highlighted the need to "counter a range of threats posed by hacking, computer viruses, and other malicious acts." A recent Center for Strategic and International Studies report on Russian targeting of the judiciary's system notes, "[t]here is an immediate need to expand both the content and the reach of threat awareness among practitioners in the justice system so that they are cognizant of the threat and can be ready to respond."
- Adversaries abroad have similarly targeted Congress, most recently documented in a number of attempted hacks of Senate offices. This threat goes back over a decade, with one notable incident in 2008 impacting a number of Congressional computers. These adversaries are likely are using every tool at their disposal to compromise the ICT used every day by Congressional offices, committees, and staff.

The Senators claimed that "Congress created the FASC to advance a critical information-sharing mission that includes identifying criteria for sharing information with both federal agencies and non-federal entities...[and] [t]o ensure that the federal government maintains a true whole-of-government SCRM policy in line with Congressional intent, we urge the FASC to develop a strategic plan that will specifically incorporate information sharing with the judiciary and Congress." The Senators stated that "[a]s such, we request that FASC provide information to the Senate Sergeant at Arms, the House of Representatives Chief Information Officer, and their appropriate counterparts in the Judiciary that includes, but is not limited to, threat briefings on ICT." They ask for a written response by October 23, 2019.

A fair reading of the bill that created and directed the FASC, the "Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act" (SECURE Act) (P.L. 115-390), would allow the FASC to develop means of sharing information with the two other branches of the federal government regarding ICT SCRM. However, were the Trump Administration to decline to read the statute that way, Congress could act in a number of ways. Presumably if OMB were to balk at looping in Congress and the federal judiciary, Congress could pass legislation to expand the purview of FASC, maybe by tacking it onto an NDAA or appropriations bill. Language could always be tucked into a committee report as well.

Further Reading

- "China Masters Political Propaganda for the Instagram Age" – *The New York Times*. The regime in Beijing has learned more effective techniques to inculcate patriotism and belief in the Communist Party than their forebearers used, including prompting studios to make more appealing films about recent Chinese history, coopting popular cartoons, and developing apps. Of course, restricting access to the internet the rest of the world sees and tirelessly monitoring and policing social media also help.
- "How Tim Cook Won Donald Trump's Ear" – *The Wall Street Journal*. Savvy moves by Apple CEO Tim Cook and Apple have kept him and the company he leads free from Presidential barbs on Twitter and have resulted in key Apple goods being exempted from tariffs on Chinese imports even though Cook support former Secretary of State Hillary Clinton and 97% of Apple employee political donations went to the Democrats in 2018.
- "France set to roll out nationwide facial recognition ID programme" – *South China Morning Post*. President Emmanuel Macron is pushing France to be the first EU nation to use facial recognition technology to enroll all citizens in a national digital identity program, Alicem, starting as early as next month. The plan is being challenged in court, France's data protection authority is concerned the program violates the General Data Protection

Regulation, and it was hacked an hour after being announced in April. Even though the Interior Ministry says the initial facial scans will be deleted and not used to monitor people, there is opposition. Since February, the city of Nice has been running trials of a facial recognition system on its CCTV system. Nonetheless, this may the start of a trend in Europe because the new European Union Commission has articulated plans to use facial recognition technology, and a British court rejected a challenge to the use of the technology by police in South Wales to make real time identifications.

- "India Is Creating A National Facial Recognition System, And Critics Are Afraid Of What Will Happen Next" – *BuzzFeed News*. India is also well on its way to a pervasive surveillance state through the increasing use of facial recognition technology and linking disparate data bases. Critics of the Modi regime argue that safety and security policy rationales are ruses for surveilling Minorities, especially Muslims, and anyone opposed to the right-wing government.
- "Tim Cook defends pulling Hong Kong app, echoing police view" – *Bloomberg*. Under pressure from China's government, Apple removed HKmap.live from its App Store that Hong Kong protestors had been using to track the real time location and activities of police. In a memo leaked to Bloomberg, Cook claimed "Over the past several days we received credible information, from the Hong Kong Cybersecurity and Technology Crime Bureau, as well as from users in Hong Kong, that the app was being used maliciously to target individual officers for violence and to victimize individuals and property where no police are present." China is Apple's number two market, and its decision to remove the Taiwanese flag from available emojis on its devices suggests the company is most interested in appeasing Beijing. *See also* "China criticizes Apple for app that tracks Hong Kong police" – *AP*.
- "Surveillance contractor that violated rules by copying traveler images, license plates can continue to work with CBP" – *The Washington Post*. Even though it violated Customs and Border Protection's rules on handling sensitive information, a contractor whose trove of license plate data was hacked last month can continue contracting with CPB subject to specified requirements going forward. Perceptics kept copies of license plates and travelers on its systems in violation of its agreement with CPB.
- "Political Campaigns Know Where You've Been. They're Tracking Your Phone." – *Wall Street Journal*. The political world is now tapping into the treasure trove of information the apps on your smartphone are broadcasting and monetizing day and night. A particularly effective use is to identify potential voters by those who attend rallies or church.
- "NSA director rebukes Beijing for 'weaponizing' disinformation in Hong Kong protests" – *cyberscoop*. General Paul Nakasone calls out the People's Republic of China for waging an information campaign against protestors in Hong Kong that bears similarities to other, external campaigns.
- "Hong Kong protesters get pro bono cybersecurity help from Silicon Valley" – *MIT Technology Review*. A U.S. company provided 500 security keys to protestors to fend off Chinese attempts to hack and take over accounts. These are the same type of security keys Google has started using, which they claim have functioned as 100% effective and safe multi-factor authentication.
- "Marco Rubio seeks U.S. government probe of TikTok over Chinese censorship concerns" – *The Washington Post*. Florida's senior Senator and one-time presidential candidate is asking the Department of the Treasury to investigate Bytedance which turned music.ly into Tik Tok, an app with over 1 billion users. Rubio wants the agency to use its CFIUS powers to delve into the company's suppression of free speech, particularly related to the unrest in Hong Kong.

- "How Telegram Became White Nationalists' Go-To Messaging Platform" – *Vice News*. Favored by ISIS, Telegram, an end-to-end encrypted messaging app has become home to many white supremacists who can no longer use 8chan. White supremacists are utilizing the app's capacity for unlimited uploads of photos and videos to private channels that critics claim is far more violent and threatening than on other platforms.