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

Spotlight: A Privacy Bill A Week

This week, we will look at a pair of bills referenced by Senate Banking, Housing, and Urban Affairs Committee Chair Mike Crapo (R-ID) at a hearing on data ownership that take a different approach to privacy. In short, these bills would approach the issues presented by mass collection and use of consumer data by granting ownership rights.

Senator John Kennedy (R-LA) introduced the "Own Your Own Data Act" (S. 806), and Senators Mark Warner (D-VA) and Josh Hawley (R-MO) introduced the "Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data" (S. 1951).

The "Own Your Own Data Act" provides that "[e]ach individual owns and has an exclusive property right in the data that an individual generates on the internet under section 5 of the Federal Trade Commission Act." This provision of a new right raises many more questions than it answers. Presumably, the required rulemaking the Federal Trade Commission (FTC) must undertake to effectuate this language will fill some gaps and define the terms that this brief three-page bill does not.

Additionally, every "social media company," a term not defined by the bill, must

- have a prominently and conspicuously displayed icon each user may click to obtain a copy of the user's data with any analysis of the user's data performed by the social media company;
- have a prominently and conspicuously displayed icon each user may click to easily export the user's data with any analysis of the user's data performed by the social media company.

These provisions would seem to lend themselves to greater transparency in how one's personal data is being used and portability should someone want to use a different platform.

The key provision of the bill, however, is that every user of a social media company's offerings must "knowingly and willfully enter into a licensing agreement" during the registration of the account. For future users this legislation would grant them the ability to license the exclusive property that is their data, but what of existing accounts such as the millions of Facebook, Twitter, and Google accounts in the U.S.? Would this be only prospective as legislation typically is? And, if so, then current users of Twitter, and Facebook may not be able to license their accounts as the companies might not need to offer them the opportunity. As a practical matter, these companies might offer current users the opportunity, but within the four corners of the bill, they would be under no obligation to do so.

The FTC would be able to enforce this act. However, it is not altogether clear how the FTC would enforce this act. Would the misuse or stealing of a person's personal data be considered a violation of the Section 5 prohibition on unfair and deceptive practices? Will the FTC's required rulemaking deem a violation of one's exclusive property right in their personal data a violation of the Section 5 bar against deceptive and unfair practices? Or is the FTC to wade into enforcing personal licenses

and punishing violations? Would the agency husband its resources and wait until it has a sizeable number of complaints about social media company X before it investigates? This may be a likely outcome given that a number of critics of the FTC already claim the agency is stretched too thin and brings too few enforcement actions for data security and privacy violations.

Regarding the rulemaking, the FTC "promulgate regulations carrying out this [bill], which shall be approved by Congress." Presumably the agency must use the more cumbersome Moss-Magnuson procedures for rulemaking instead of the Administrative Procedure Act (APA) notice and comment process? However, the bill does not speak directly this point, and so it is likely the FTC would be stuck using the Moss-Magnuson process which has effectively choked off the agency's rulemaking capability.

How exactly will Congress must approve these regulations? Will it be like reprogramming requests that usually require the assent of the Appropriations Committees often through a formal process? Or will the informal sign off from the committees of jurisdiction over the FTC suffice? Or must Congress pass a resolution of approval or disapproval as it may under a number of statutes designed to police executive branch actions? The bill leaves this question unanswered.

A different privacy bill we examined, the "American Data Dissemination (ADD) Act" (S. 142) also requires the FTC to submit regulations to Congress. In the case of that bill, the agency needs to send "detailed recommendations [to the House Energy and Commerce Committee and the Senate Commerce, Science, and Transportation Committee] for privacy requirements that Congress could impose on covered providers that would be substantially similar, to the extent practicable, to the requirements applicable to agencies under the Privacy Act of 1974." 12-15 months after the FTC submits this report, it would be required to submit to the same committees proposed regulations that would similarly make covered entities subject to requirements along the lines of how the Privacy Act of 1974 applies to federal agencies.

However, despite creating a property right, there is no right of action provided by the bill. Consumers would not be able to sue if their licensing of their "exclusive property right in the data" they generate is violated. Normally, for most property rights, consumers may go to court if they think their rights to this property have been impinged. This bill would not grant such a right to consumers, and I do not know of any other federal grounds under which consumers would be able to sue. Or would a person's data be similar to trademarked or copyrighted information? Among the many questions raised under this scheme, would consumers be able to use existing state property statutes to sue in state courts? Could a state like California enact a right to sue for a violation of this newly created federal right?

This week's other bill, the "Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data" (S. 1951), would force a select class of online entities to disclose how much they earn from users' data and also provide consumers the right to delete their data subject to some exceptions. The entities would need to file additional disclosures with the Securities and Exchange Commission (SEC) to bring greater transparency to consumers, shareholders, and investors regarding the value of the data that companies collect and then share.

The bill defines which companies or entities would be "commercial data operators" those "acting in its capacity as a consumer online services provider or data broker that—

- generates a material amount of revenue from the use, collection, processing, sale, or sharing of the user data; and

- has more than 100,000,000 unique monthly visitors or users in the United States for a majority of months during the previous 1-year period."

This definition would seem to include a small class of online entities while excluding most businesses that generate a material amount of their revenue from other activities. But, how "material" is defined would determine how a company like an auto manufacturer that derives significant revenue from both auto sales and the sale or sharing of personal data would be treated. Nonetheless, those entities that act as data brokers would be swept into this definition of commercial data operators, and they would need to meet the new responsibilities imposed on them.

Generally, the bill would require every commercial data operator to "provide each user of the commercial data operator with an assessment of the economic value that the commercial data operator places on the data of that user." The agency charged with effectuating this portion of the bill, the FTC, would likely need to spell out what constitutes an "assessment of economic value." Would this need to be consumer friendly and easily understandable?

Additionally, commercial data operators would have to reveal to all users the following

- the types of data collected from users of the commercial data operator, whether by the commercial data operator or another person pursuant to an agreement with the commercial data operator; and
- the ways that the data of a user of the commercial data operator is used if the use is not directly or exclusively related to the online service that the commercial data operator provides to the user

These disclosures seems straightforward and seem designed to better inform consumers about all the sources from which a commercial data operator is obtaining data and all the additional uses of user data beyond those immediate uses of the commercial data operator. Again, how this information is presented to consumers would be key, for if the format is barely intelligible or a sprawling spreadsheet, then one wonders how much the average use of Twitter would understand it. Additionally, would the FTC be able to aggregate these data and publish de-identified statistics on industry-wide data usage practices for commercial data operators? It would appear so. Additionally, the filings that must be made to the SEC would seem to present the FTC and the Department of Justice with a new source of data to investigate possible anti-competitive activity in the markets where commercial data operators are present.

Users must also be able to delete all the data a commercial data operator possesses subject to certain exceptions by the use of "a single setting" or "another clear and conspicuous mechanism by which the user may make such a deletion." The excepted circumstances under which deletion may not occur are

- in cases where there is a legal obligation of the commercial data operator to maintain the data;
- for the establishment, exercise, or defense of legal claims; or
- if the data is necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or assist in the prosecution of those responsible for such activity.

However, commercial data operators may not retain any more user data than is necessary to "carry out" the aforementioned exceptions to the general right of users to delete their data. This would seem to serve as a limit to an entity's likely inclination to interpret such restrictions in ways most

favorable to them. However, the extent to which these companies did not push the boundaries egregiously will hinge on FTC enforcement.

As mentioned, the FTC would enforce this new regime. Like virtually all the other privacy bills, the FTC would be empowered to treat acts contrary to the bill "as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act," meaning the ability right off the bat to ask federal courts for civil fines of more than $40,000 per violation in addition to all the other enforcement tools the FTC normally wields in data security and privacy cases. Of course, the full panoply of the FTC's other powers would still be available for such cases.

In a twist for a privacy bill, commercial data operators would need "to file an annual or quarterly report" with the SEC that must disclose" the aggregate value, if material, of—

- user data that the commercial data operator holds;
- contracts with third parties for the collection of user data through the online service provided by the commercial data operator; and
- any other item that the [SEC] determines, by rule, is necessary or useful for the protection of investors and in the public interest.

The SEC must also "develop a method or methods for calculating the value of user data required to be disclosed" and "provide quantitative and qualitative disclosures about the value of user data held" by some commercial data operators."

These data disclosure requirements would likely bring much greater transparency into the data practices of a company like Facebook or Google, presumably allowing investors to better understand and value such companies. In a section-by-section summary, Warner and Hawley asserted two additional ways the bill would address data privacy and usage:

- making the value more transparent could increase competition by attracting competitors to the market.
- disclosing the economic value of consumer data will also assist antitrust enforcers in identifying unfair transactions and anticompetitive transactions and practices.

While these two bills take different approaches on data privacy by trying to leverage the economics of data, it is not clear how appealing these are to Democrats whose agreement will be needed before any privacy leverage can move forward. Possibly a modified version of the concepts in these bills could be added to a broader privacy bill such that entities collecting and sharing data would need to make additional disclosures to the SEC.

Democrats Again Push Election Security Bills

The House took up and passed its third bill on election security this year, the "Stopping Harmful Interference in Elections for a Lasting Democracy Act" (SHIELD Act) (H.R. 4617), that addresses two of the technological facets of foreign disinformation campaigns aimed at U.S. elections according to the House Administration Committee's summary:

- Helps prevent foreign interference in future elections by improving transparency of online political advertisements.
    - Russia attempted to influence the 2016 presidential election by buying and placing political ads on platforms such as Facebook, Twitter and Google. The content and purchasers of those online advertisements were a mystery to the public because of

outdated laws that have failed to keep up with evolving technology. The SHIELD Act takes steps to prevent hidden, foreign disinformation campaigns in our elections by ensuring that political ads sold online are covered by the same rules as ads sold on TV, radio, and satellite.

- Prohibits deceptive practices about voting procedures.
    - Independent experts have identified voter suppression tactics the Russians used on social media, including malicious misdirection designed to create confusion about voting rules. The SHIELD Act incorporates the Deceptive Practices and Voter Intimidation Prevention Act to prohibit anyone from providing false information about voting rules and qualifications for voting, provides mechanisms for disseminating correct information, and establishes strong penalties for voter intimidation.

The House passed H.R. 4617 by a 227-181 vote with all Republicans present voting no and one Democrat joining them.

House Democrats seem intent on making the security and safety of elections a part of their legislative program despite dim prospects in the Senate where Senate Majority Leader Mitch McConnell (R-KY) has said he will not bring any such legislation to the floor.

In February, the House passed "For The People Act of 2019" (H.R. 1) on a party-line vote, which included a process by which cybersecurity standards would be established for election infrastructure vendors and would also authorize grants for states and localities to upgrade and secure their election systems. For example, "qualified election infrastructure vendors" must agree "to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee" and to promptly report cybersecurity incidents to the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC).

In late June, the House considered and passed the "Securing America's Federal Elections (SAFE) Act of 2019" (H.R. 2722) also largely along a party-line vote. In the Committee Report, the House Administration Committee explained the bill:

- H.R. 2722 provides critical resources to states and localities to bolster election infrastructure, including necessary funds to replace aging voting equipment with voter-verified paper ballot voting systems and implement additional cybersecurity protocols. The bill also helps states and localities plan for future elections by providing ongoing maintenance funding on a biannual basis. The legislation provides grant programs for states to implement required risk-limiting audits, a best practice audit system that confirms election outcomes with a high degree of confidence.
- The legislation also institutes accountability for election technology vendors so that they abide by cybersecurity standards, including agreeing to report known or suspect security incidents involving election infrastructure.

In the Senate this week, Democrats tried to bring election security legislation to the floor despite the opposition of McConnell and other Republicans. On October 22, Amy Klobuchar (D-MN) and Senate Minority Whip Dick Durbin (D-IL) each asked for unanimous consent to bring up election security legislation, and they, too, were blocked by objections lodged by Republicans. Klobuchar wanted to bring forward her bill, "Honest Ads Act" (S. 1356), which, according to her press release

upon introduction, "enhances the integrity of our democracy by improving disclosure requirements for online political advertisements by:

- Amending the Bipartisan Campaign Reform Act of 2002's definition of electioneering communication to include paid Internet and digital advertisements.
- Requiring digital platforms with at least 50,000,000 monthly viewers to maintain a public file of all electioneering communications purchased by a person or group who spends more than $500.00 total on ads published on their platform. The file would contain a digital copy of the advertisement, a description of the audience the advertisement targets, the number of views generated, the dates and times of publication, the rates charged, and the contact information of the purchaser.
- Requiring online platforms to make all reasonable efforts to ensure that foreign individuals and entities are not purchasing political advertisements in order to influence the American electorate."

Durbin's consent request to bring another Klobuchar bill, the "Election Security Act" (S. 1540), directly to the Senate floor was also blocked. Durbin claimed the bill "would provide critical resources to election officials through an initial $1 billion investment in our election infrastructure, followed by $175 million every 2 years for infra-structure maintenance…[and] would also require the use of voter-verified paper ballots, strengthen the Federal response to election interference, and establish accountability measures for election technology vendors."

On October 23, Senators Mark Warner (D-VA), Klobuchar, and Ron Wyden (D-OR) made unanimous consent requests to bring to the floor the following bills:

- The "Foreign Influence Reporting in Elections Act" (S. 2242)
- S. 2669, A bill to amend the Federal Election Campaign Act of 1971 to clarify the obligation to report acts of foreign election influence and require implementation of compliance and reporting systems by Federal campaigns to detect and report such acts, and for other purposes.
- The "Securing America's Federal Elections Act" (SAFE Act) (S. 2238)

However, Senator Marsha Blackburn (R-TN) objected to each request.

House Homeland Security Marks Up A Pair of Tech Bills

On October 23, 2019 the House Homeland Security Committee held a markup and approved the a pair of cybersecurity-related bills en bloc with other legislation, as amended, by voice vote:

- The "Advancing Cybersecurity Diagnostics and Mitigation Act" (H.R. 4237)
- The "National Commission on Online Platforms and Homeland Security Act" (H.R. 4782)

The "Advancing Cybersecurity Diagnostics and Mitigation Act" (H.R. 4237) would codify the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program and charge DHS with executing the following duties:

> (i) assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities;
> (ii) develop and provide the capability to collect, analyze, and visualize in- formation relating to security data and cybersecurity risks at agencies;
> (iii) make program capabilities available for use, with or without reimbursement, to civilian agencies and State, local, Tribal, and territorial governments;

(iv) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;
(v) assist entities in setting information security priorities and assessing and managing cybersecurity risks; and
(vi) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

Moreover, "each agency that uses the CDM program…shall, continuously and in real time, provide to the Secretary all information, assessments, analyses, and raw data collected by the program, in a manner specified by" DHS. Additionally, DHS "shall develop a comprehensive CDM strategy to carry out the continuous diagnostics and mitigation program." DHS must also "a report on cybersecurity risk posture based on the data collected through the CDM program" to the Homeland Security Committees.

This bill faces an uncertain fate in the Senate. In 2018, the House passed a similar bill, H.R. 6443, also named the "Advancing Cybersecurity Diagnostics and Mitigation Act," which never made it out of the Senate Homeland Security and Governmental Affairs Committee.

The "National Commission on Online Platforms and Homeland Security Act" (H.R. 4782) would create a 12-member National Commission on Online Platforms and Homeland Security that would examine issues related to online domestic and international terrorism, foreign interference and disinformation practices in light of civil liberties and Constitutional rights and then deliver recommendations on how online platforms could better police their sites and apps. An interim report would due to Congress within one year of enactment, and then a final report in two years that must address the following:

- Policy mechanisms that would address the Commission's findings in a manner that promotes free speech and innovation on the internet, preserves individual privacy, civil rights, and civil liberties, and upholds the principles of the Constitution.
- Policies and procedures that owners or operators of online platforms could implement to address such areas of study that preserve the individual privacy, civil rights, and civil liberties of online platform users.
- Mechanisms to improve transparency and accountability related to the matters described in subsection (g) [i.e. current platform practices], including any best practices identified pursuant to paragraph (3) of such subsection.
- Areas with respect to which additional research is required, informed by the evaluation of prior research…
- Other matters identified by the majority of Commission members.

The Under Secretary of Homeland Security for Science and Technology must collect and analyze existing research on "previous acts of targeted violence, including domestic terrorism or international terrorism" and undertake research "to better understand whether any connection exists between the use of online platforms, particularly platforms used for social media and social networking, and targeted violence, including domestic terrorism and international terrorism." The Under Secretary must also "develop voluntary approaches that could be adopted by owners and operators of online platforms to address research findings…while preserving the individual privacy, civil rights, and civil liberties of users."

In a fact sheet, the committee stated:

> As terrorists livestream their attacks via services like Facebook Live and post their hateful manifestos online on sites like 8chan, online platforms have struggled to respond to the speed and scale of viral terrorist content. They have also struggled to effectively address covert malign activity by foreign nation states to interfere with U.S. elections. [This legislation is necessary in order] [t]o better understand the degree to which online platform have been exploited to carry out such activity and develop voluntary approaches that platforms could utilize to address such concerns while promoting free speech and innovation on the internet.

This bill was scheduled for a markup last month but was pulled amidst concerns from civil liberties and privacy advocates. However, the reaction to the revised bill was lukewarm. The Center for Democracy and Technology (CDT) stated:

> Various iterations of the bill have circulated and been reported on while civil liberties groups, CDT included, have raised concerns about the scope of the bill, its broad subpoena power, and the implications of its charter for online privacy and free expression. In response, the bill has been revised several times and with each iteration has come to better enshrine protections for these fundamental rights. The latest version of the bill comes much closer to achieving these goals than any prior drafts, including privacy and free expression as core elements of the Commission's mandate.

CDT added

- The bill is still lacking in a few areas. While the scope of the Commission's work has been narrowed it still covers two, if not three distinct areas: domestic/international terrorism and foreign influence campaigns. These topics are (and should be) of interest to Congress, however, they are also topics that are separate from each other: at major online platforms, their challenges are largely tackled by different teams, their effect on internet users' and their online experiences wholly distinct, and their influence on the democratic process very different. Ultimately, the Commission may be out of its depth trying to tackle such disparate issues.
- Also concerning are the Commission's mandates to explore how and whether platforms "have been able to respond effectively" to threats of targeted violence and foreign influence campaigns, and how and whether they "consistently and effectively enforce" policies to limit those threats. It's unclear how the Commission plans to evaluate platforms' consistency and effectiveness.

Mark Zuckerberg Appears Before House Committee

Last week, the House Financial Services Committee heard testimony from Facebook CEO and Founder Mark Zuckerberg at its hearing on the impact of Facebook on housing and financial services over the course of an often contentious five hour hearing that covered virtually all lawmakers' concerns about the company in particular and social media in general. The chair even suggested that breaking up Facebook is the best course of action, thus echoing a number of contenders for the Democratic nomination for the presidency. Zuckerberg's responses balanced contrition for some of Facebook's previous conduct with promises of better behavior in the future.

In its memorandum for the hearing, the majority staff explained:

> On June 18, 2019, Facebook announced its plans to develop a new cryptocurrency, called Libra, and a digital wallet to store this cryptocurrency, called Calibra. Libra will be built on blockchain, backed by a reserve of assets, and governed by the Libra Association. The Libra Association (Association), which, at that time, was comprised of Facebook and 27 other members, is an independent, not-for-profit organization headquartered in Geneva, Switzerland. Its members will verify Libra transactions within the Libra blockchain. Facebook hopes to have recruited over 100 firms into the Association by the target launch date of early 2020.

Staff added:

- As the first step in the Congressional process, on July 17, 2019, the Committee held a hearing to hear directly from the architect of this project, David Marcus, the Chief Executive Officer of Calibra, as well as, other cryptocurrency experts. As discussed during that hearing and in the accompanying materials, Facebook's plans have serious implications for investors, consumers, data privacy, cybersecurity, systemic risks, monetary policy, and national security.
- Moreover, as part of the hearing, the Independent Community Bankers of America's (ICBA) submitted a letter to the Committee, writing, "The proposed creation of Libra, if allowed to proceed, would be a significant and irreversible development that would alter the global financial landscape." ICBA also noted its support for a moratorium on the implementation of Libra and expressed concerns about financial stability, given that Libra could be prone to bank-like runs without any comparable deposit insurance system.
- U.S. regulators have also raised concerns with Libra. According to Federal Reserve Board Chairman Jerome Powell, "Libra raises many serious concerns regarding privacy, money laundering, consumer protection, and financial stability." Chairman Powell stated that the project "cannot go forward" without addressing those concerns.
- President Trump and Treasury Secretary Mnuchin raised similar concerns. Likewise, Federal Reserve Board Governor Lael Brainard has stated that "there are likely to be financial stability risks for a stablecoin network with global reach. If not managed effectively, liquidity, credit, market, or operational risks—alone or in combination—could trigger a loss of confidence and a classic run." In August, regulators from France and Germany both agreed to block Libra from their countries; in a joint statement, the two governments stated that "no private company can claim monetary power, which is inherent to the sovereignty of nations." The G-7 and the Financial Stability Board (FSB) called for more scrutiny and high regulatory standards for stablecoins, such as Libra, particularly to protect consumers and ensure cryptocurrencies are not used to launder money or fund terrorism.

Chair Maxine Waters (D-CA) stated that "Facebook's plans to create a digital currency, Libra, and a digital wallet, Calibra, raise many concerns relating to privacy, trading risks, discrimination, opportunities for diverse-owned financial firms, national security, monetary policy, and the stability of the global financial system." She note that "I and other Democrats have called for a moratorium on Facebook's development of its digital currency, Libra, and digital wallet, Calibra until Congress can examine the issues associated with a big tech company developing these digital products and take action." Waters explained that "[a]s I have examined Facebook's various problems, I have come to the conclusion that it would be beneficial for all if Facebook concentrates on addressing its many existing deficiencies and failures before proceeding any further on the Libra project."

Waters said to Zuckerberg "[l]et's review your record:

- **On diversity and inclusion,** Facebook has utterly failed. Facebook's executive ranks and workforce continue to be mostly white and male. Since Reverend Jesse Jackson and the Rainbow PUSH Coalition called upon Silicon Valley companies including Facebook to release diversity statistics more than five years ago, the representation of African Americans and Hispanics has increased by less than two percent. Facebook also told us that they have zero dollars managed by diverse firms.
- **On fair housing,** Facebook has been sued by the National Fair Housing Alliance for enabling advertisers to engage in discrimination on its advertising platforms. The U.S. Department of Housing and Urban Development (HUD) has also filed an official charge of discrimination against Facebook for its advertising practices, including the company's own ad delivery algorithms, which were found to have a discriminatory impact even when advertisers did not target their audience in discriminatory ways. I understand that Facebook has refused to cooperate with HUD's fair housing investigation by refusing to provide relevant data.
- **On competition and fairness,** Facebook is the subject of an antitrust investigation by the Attorneys General of 47 states and the District of Columbia.
- **On protecting consumers,** Facebook was fined $5 billion by the Federal Trade Commission for deceiving consumers and failing to keep their data private.
- **On elections,** Facebook enabled the Russian government to interfere with our election in 2016 with ads designed to pit Americans against each other, suppress the vote and boost Trump. For example, Facebook allowed a counterfeit Black Lives Matter webpage to operate with the goal of discouraging African Americans from voting. Three years later these activities are still continuing on Facebook. We learned just this week that Russia and Iran are using the same tactics to meddle in our next election.
- **On political speech**, last week, you announced that Facebook would not be doing fact-checking on political ads, giving anyone Facebook labels a politician a platform to lie, mislead and misinform the American people, which will also allow Facebook to sell more ads. The impact of this will be a massive voter suppression effort that will move at the speed of a click. Your claim to promote freedom of speech does not ring true.

Water added "Mr. Zuckerberg, each month, 2.7 billion people use your products…over a third of the world's population." She asserted that "[t]hat's so big that it's clear to me and to anyone who hears this list, that you believe that you are above the law, and it appears that you are aggressively increasing the size of your company, and are willing to step on or over anyone-- including your competitors, women, people of color, your own users, and even our democracy-- to get what you want." Waters contended that "[w]ith all of these problems I have outlined, and given the company's size and reach, it should be clear why we have serious concerns about your plans to establish a global digital currency that would challenge the U.S. dollar." She declared "[i]n fact, you have opened up a serious discussion about whether Facebook should be broken up."

Ranking Member Patrick McHenry (R-NC) claimed that "[t]oday is a trial on American innovation." He conceded that "[t]here's a growing concern about the role that technology plays in our lives…[and] [y]es, technology has led to greater prosperity, more freedom of expression, and the ability to transcend the limits of space and time to connect us with one another." McHenry said that "we know there's also a downside to all of this….[t]he vitriol on social media is frightening…[t]he growing inequality between those who have access to the latest tech gadgets remain on the coasts, while folks living in rural America are still trying to get basic access to the internet." He added "[n]ot to mention the anxiety of this age, that nervous feeling of needing to check your phone throughout

the day." McHenry claimed that "[t]here's a lot of anger out there, and it's now being directed at the architects of this system…[and] [t]hat's why you're here today Mr. Zuckerberg."

McHenry stated that "[t]his is not just about Libra, not just about some bad housing ads, and maybe not really about Facebook at all." He asserted that "[y]ou are here as one of the titans of this new era that we call the digital age…[a]nd fair or not, you are here today to answer for it." McHenry explained that "of course, you are not America's first innovator, and this is not the first time that America has faced difficult questions about technology." He stated that "[s]adly, throughout the history of innovation, a major theme is the exploitation of fear…[and] [p]oliticians, enabled by special interests and a lack of understanding of new technology, use fear to justify what is ultimately a power grab…[n]ew laws…[n]ew regulation…[b]ut ultimately, old and tired ways to centralize power here in Washington."

McHenry contended that "[s]ome of this has led to comical results." He said that "[t]here was time when legislators pushed for so-called 'red flag' laws, which required vehicles, called 'horseless carriages,' to immediately stop on the side of the road and disassemble the automobile until 'equestrian or livestock was sufficiently pacified.'" McHenry noted that "other times in history the use of fear was not so funny" and during "[o]ur last hearing on Libra, for example, was a moment where a member of Congress actually compared the technology to September 11th."

McHenry allowed that "I have my own qualms about Facebook and Libra and the shortcomings of Big Tech…[t]here are many." He stated that "if history has taught us anything, it's better to be on the side of American innovation, competition, and most importantly the freedom to build a better future for all of us…[and] [p]rogress is not preordained." McHenry claimed that "[l]et us not forget that the wave of innovation is spreading across the world—with or without us…[and] [s]o that is why I believe American innovation is on trial today." He stated that "the question is: Are we going to spend our time trying to devise ways for government planners to centralize power and control as to who, when, and how innovators can innovate, or are we going to spend our time building a brighter future for America together?"

Facebook CEO and Founder Mark Zuckerberg stated:

- There are more than a billion people around the world who don't have access to a bank account, but could through mobile phones if the right system existed. This includes 14 million people here in the US. Being shut out of the financial system has real consequences for people's lives—and it' s often the most disadvantaged people who pay the highest price.
- People pay far too high a cost—and have to wait far too long—to send money home to their families abroad. The current system is failing them. The financial industry is stagnant and there is no digital financial architecture to support the innovation we need. I believe this problem can be solved, and Libra can help. The idea behind Libra is that sending money should be as easy and secure as sending a text message. Libra will be a global payments system, fully backed by a reserve of cash and other highly liquid assets.
- I believe this is something that needs to get built, but I understand we're not the ideal messenger right now. We've faced a lot of issues over the past few years, and I'm sure people wish it was anyone but Facebook putting this idea forward.
- But there's a reason we care about this. Facebook is about putting power in people's hands. Our services give people voice to express what matters to them, and to build businesses that create opportunity. Giving people control of their money is important too. A simple, secure, and stable way to transfer money is empowering. Over the long term, if it means

more people transact on our platforms, that would be good for our business. But even if it doesn't, it could help people everywhere.

- Before we move forward, there are important risks that need to be addressed. There are questions about financial stability, fighting terrorism, and more. I'm here today to discuss those risks and how we plan to address them. But I also hope we can talk about the risks of not innovating. While we debate these issues, the rest of the world isn't waiting. China is moving quickly to launch similar ideas in the coming months. Libra will be backed mostly by dollars and I believe it will extend America's financial leadership as well as our democratic values and oversight around the world. If America doesn't innovate, our financial leadership is not guaranteed.

Senate Banking Considers Data Ownership

The Senate Banking, Housing, and Urban Affairs Committee resumed its series of hearings into data privacy and security with a hearing titled "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation," which detailed a new vantage on how the U.S. government might address the myriad problems posed by mass collection and use of consumers' personal information. However, there was division among the Members regarding the efficacy of implementing a regime under which each consumer would negotiate deals with companies to use their data with some Democrats decrying such proposals as being related to enhanced notice and consent regimes. One witness pointed to valuation problems, noting that the processing of personal data was how value was added.

Chair Mike Crapo (R-ID) said that "[a]s a result of an increasingly digital economy, more personal information is available to companies than ever before." He said that "[p]rivate companies are collecting, processing, analyzing and sharing considerable data on individuals for all kinds of purposes." Crapo said that "[t]here have been many questions about what personal data is being collected, how it is being collected, with whom it is being shared and how it is being used, including in ways that affect individuals' financial lives." He stated that "[g]iven the vast amount of personal information flowing through the economy, individuals need real control over their personal data."

Crapo noted that "[t]his Committee has held a series of data privacy hearings exploring possible frameworks for facilitating privacy rights to consumers….[and] [n]early all have included references to data as a new currency or commodity." He stated that "[t]he next question, then, is who owns it?" Crapo stated that "[t]here has been much debate about the concept of data ownership, the monetary value of personal information and its potential role in data privacy." He asserted that "[s]ome have argued that privacy and control over information could benefit from applying an explicit property right to personal data, similar to owning a home or protecting intellectual property…[and yet] [o]thers contend the very nature of data is different from that of other tangible assets or goods."

Crapo stated that "[s]till, it is difficult to ignore the concept of data ownership that appears in existing data privacy frameworks." He said that "[f]or example, the European Union's General Data Protection Regulation, or GDPR, grants an individual the right to request and access personally identifiable information that has been collected about them." Crapo contended that "[t]here is an inherent element of ownership in each of these rights, and it is necessary to address some of the difficulties of ownership when certain rights are exercised, such as whether information could pertain to more than one individual, or if individual ownership applies in the concept of derived data." He

stated that "[a]ssociated with concepts about data ownership or control is the value of personal data being used in the marketplace, and the opportunities for individuals to benefit from its use."

Crapo asserted that "Senators [John] Kennedy (R-LA) and [Mark] Warner (D-VA) have both led on these issues, with Senator Kennedy introducing legislation that would grant an explicit property right over personal data (i.e. the "Own Your Own Data Act" (S. 806), and Senator Warner introducing legislation that would give consumers more information about the value of their personal data and how it is being used in the economy (i.e. the "Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data" (S. 1951)." Crapo contended that "[a]s the Banking Committee continues exploring ways to give individuals real control over their data, it is important to learn more about what relationship exists between true data ownership and individuals' degree of control over their personal information; how a property right would work for different types of personal information; how data ownership interacts with existing privacy laws, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and GDPR; and different ways that companies use personal data, how personal data could be reliably valued and what that means for privacy."

Ranking Member Sherrod Brown (D-OH) remarked that "[t]his Committee has spent some time over the last several months discussing Facebook's poorly thought out plan to create a global currency." He claimed that "the bottom line is that we know that Facebook can't be trusted with Americans' personal information and it is terrible at protecting its users' privacy…[so] [i]t was pretty clear the last thing we should do is trust them with American's hard-earned dollars." Brown stated that "it isn't just Facebook…[because] very time corporations in Silicon Valley come up with a new business model, the result is the same – they get more access to our personal data, spending habits, location, the websites we visit, and it means more money in their pockets." He added that "everyone else gets hurt." Brown said that "I want to begin this hearing with a simple question – who has the right to control your personal, private information: you or Silicon Valley CEOs like Mark Zuckerberg?"

Brown stated that "I think we all agree that Americans should have more control over their private information…[b]ut should we treat that private information like property?" He stated that "[a]t first glance this might seem like a simple way to tackle the complex problems created by data collection and machine learning…[and] [t]he promise is that if we just treat personal data like property, markets will do the hard work of protecting our privacy for us." Brown argued that is "not how it will work." He contended that "[i]nstead of making companies responsible for protecting their customers' privacy, this idea puts the burden on all of us." Brown stated that "imagine that if every time you wanted to use Facebook, or pay for something with an app, or login to a Wi-Fi network, you had to read even more legal fine print, and check a box saying, 'okay, I waive my personal right to my data to use this service'…[o]r you had to join some kind of so-called "data collective" to sell your data." He claimed "[w]orking people in this country have enough to worry about – they're trying to get the kids out the door and get to work on time; to make rent and save for college and pay the bills." Brown asserted that "[t]he idea that people should also have to manage their data like a landlord manages its tenants is ludicrous." Brown declared that "[t]his should be pretty simple – corporations should not be allowed to invade our privacy…[and] [w]e know that today, they are."

Brown asserted that "[b]ig tech companies don't want to protect your personal information – they want to profit off it…[and] [p]rotecting your privacy doesn't make them any money – it costs them money – so they aren't going to do it." He claimed that "[t]hey want your data, and they want to get it for free, or pay as little as possible for it…[s]o it should be no surprise that I am skeptical

when I hear of plans for Americans' data to be treated like property." Brown stated that "[i]f Americans want more control over their private information, we have to find a way to prevent corporations from mining our data and selling it to each other…[and] [c]reating a supermarket for selling away our privacy does the opposite." He declared that "[t]reating data as something that can be owned, bought, and sold doesn't solve any of these problems—especially when undermining our privacy is the business model." Brown argued that "Mark Zuckerberg and his Silicon Valley buddies want us to skip over the part where we have control over our privacy, and jump to the part where giant tech companies get to use their market power to squeeze our privacy out of us – and it would all be legal." He added "[t]hat's unacceptable."

Founding Chair of the American Bar Association Committee on Cyberspace Law Jeffrey Ritter stated that

- Privacy law reform here will surely fail if we do not incorporate something new—a legal answer to the most fundamental question: who owns digital information? For the totality of digital information, this is an enormous chasm in the evolution of the rule of law for the Digital Age. For personally identifiable information, the question is particularly relevant.
- Yes, it is identifiable, but who owns it? In many steps to advance electronic commerce, the United States has led the world, notably enabling electronic contracts and electronic signatures to be legally valid without paper. Indeed, in humankind's history, no rule of law was more rapidly incorporated into the laws of the world than the rules we helped innovate to enable digital commerce to become real. But, in privacy, we are behind.
- To re-establish this nation's leadership, privacy reform must express clear, explicit rules that establish who owns any specific digital file or record. Only then can we be successful in crafting the additional rules for acquiring, using, transferring, selling, and controlling personal data, and imposing the sanctions for violating those rules. Think about it. Every commercial system built on the rule of law—real estate, banking, consumer and industrial products, mining—begins with a commitment to define and protect the rights of the owner of the property. Yet, across all privacy law, while a data subject has many controls on the use of identifiable information, and we often speak in conversation about ownership, the legal right of ownership has not been established.
- As summarized in a recent article submitted as part of my written testimony, Germany, Japan, and the OECD are all calling for formal legal rules on data ownership, including from Chancellor Merkel herself. Japan has already published model guidelines for structuring data sharing and licensing agreements based on ownership principles. Failing to address data ownership in our privacy reforms will surely further isolate the United States from the global momentum and allow the rules for data as property to be written by others.

American Civil Liberties Union Senior Advocacy and Policy Counsel Chad Marlow contended that

- If Congress wants to pass a law that creates meaningful privacy protections for Americans - if Congress wants to pass a law so that every time Americans use the internet, or social media, or complete a commercial transaction, they do not have their personal information gathered and offered up for sale to third parties – it does not need to treat data as property to do so. In fact, passing legislation that treats data as property carries specific harms that would undermine that goal.
- The government should not be promoting privacy as a resource to be bought and sold. A growing number of state constitutions now recognize that privacy is a fundamental right, including the constitutions of the home states of this Committee's members from Arizona, Hawaii, Louisiana, Montana, and South Carolina, along with many others.

- The proper response to the pervasive loss of individual privacy is to pass stronger privacy laws, not just to throw up our hands and conclude the only issue left to tackle is who gets the money when people's data is sold. Yes, privacy protections for personal information are weak in this country, but Congress and the states have the ability to strengthen them. And they should. Limiting data collection, retention, and further transfers without a person's clear, distinct, and informed permission is a strong place to start.
- Additionally, companies should be prohibited from denying a good or service to someone who chooses to exercise their privacy rights, and consumers should have a private right of action to seek compensation when their privacy rights are violated. Most relevant to today's discussion, we should not be looking to a data as property model, which monetarily incentivizes people to give up their privacy, to enhance privacy protections.
- Again, if those who support the data as property model want to talk about it as a potential way to create a more robust and equitable marketplace for the sale of personal data, by all means they should make that argument, but they need to stop advancing the false narrative that the data as property model is pro-privacy.

American Action Forum Director of Technology and Innovation Policy Will Rinehart stated that "[l]ike many privacy experts, I'm skeptical that data property rights are the best policy mechanism for ensuring privacy is secured in the digital age. I hope to make three main points today:

- A property right to personal data isn't needed to establish consumer privacy rights, nor would it be economically efficient to establish this kind of property right;
- Valuing personal data is difficult because raw or personal data per se is not what is in demand, but rather the insights that can be gleaned from that data—insights that often depend on the data's environment; and
- Regardless of the particular policy mechanism, privacy laws will create unavoidable costs from compliance, which will impact investment opportunities in countless industries.

EC Signs Off On Privacy Shield Despite Concerns Ahead of Possible Adverse Court Rulings

As part of the annual review process, the European Commission (EC) has released its third assessment of the U.S.-EU Privacy Shield Agreement that governs the transfer of the personal data of European Union (EU) citizens out of the EU for processing, and for the most part it finds that the agreement is working as intended. However, the EC noted the U.S. privacy and surveillance policy developments it is tracking and suggested its preferred policy outcomes on some of these matters. EU officials had met with Department of Commerce officials in mid-September for their joint annual review of the Privacy Shield, that included Director-General for Justice and Consumers Tiina Astola, Secretary of Commerce Wilbur Ross, Federal Trade Commission Chair Joe Simons, EU Commissioner for Justice, Consumers, and Gender Equality Věra Jourová, and European Data Protection Board Vice Chair Ventsislav Karadjov. The EC's report flows from this meeting.

In its press release, the EC claimed

> The report confirms that the U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the U.S. Since the second annual review, there have been a number of improvements in the functioning of the framework, as well as appointments to key oversight and redress bodies, such as the Privacy Shield Ombudsperson. Being in the third year of the Shield's operation, the review focused on the lessons learnt from its practical implementation and day-to-day functionality.

Last year the EU's threats to pull out of Privacy Shield unless the Trump Administration named a full complement of members to the Privacy and Civil Liberties Oversight Board (PCLOB) and a Privacy Shield Ombudsman resulted in nominations and Senate confirmation for those positions. In this review, there are no such open threats but more veiled suggestions about how the Trump Administration could better safeguard the administration of Privacy Shield and the personal data of EU citizens from objectionable intelligence activities.

The EC "concludes that a number of concrete steps need to be taken to better ensure the effective functioning of the Privacy Shield in practice:

> 1. The Department of Commerce should shorten the different time periods that are granted to companies for completing the re-certification process. A period of maximum 30 days in total would seem reasonable to allow companies sufficient time for re-certification, including for rectifying any issue identified in the re-certification process, while at the same time ensuring the effectiveness of this process. If at the end of this period the re-certification is not completed, the Department of Commerce should send out the warning letter without further delay.
> 2. In the context of its spot-check procedure, the Department of Commerce should assess companies' compliance with the Accountability for Onward Transfers Principle, including by making use of the possibility provided by the Privacy Shield to request a summary or a representative copy of the privacy provisions of a contract concluded by a Privacy Shield-certified company for the purposes of onward transfer.
> 3. As a matter of priority, the Department of Commerce should develop tools for detecting false claims of participation in the Privacy Shield from companies that have never applied for certification, and use these tools in a regular and systematic manner.
> 4. The Federal Trade Commission should, as a matter of priority, find ways to share meaningful information on ongoing investigations with the Commission, as well as with EU Data Protection Authorities that also have enforcement responsibilities under the Privacy Shield.
> 5. The EU Data Protection Authorities, the Department of Commerce and the Federal Trade Commission should develop common guidance on the definition and treatment of human resources data in the coming months.

Notably, the EC is calling on the FTC to ways to better share information with the EU's data protection authorities regarding "ongoing investigation." However, it is not clear whether this refers only to Privacy Shield investigations or to broader investigations regarding possible anti-trust, data security, and/or privacy violations. Of course, the FTC has statutory authorization to cooperate with foreign agency counterparts under the "Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006" (P.L. 109-455).

The EC stated it "will continue to closely monitor further developments concerning specific elements of the Privacy Shield framework, notably

> (i) the functioning of the Ombudsperson mechanism, in particular in case of a new complaint;
> (ii) the outcome of the ongoing oversight projects that have been initiated by the Privacy and Civil Liberties Oversight Board and that are particularly relevant for the Privacy Shield (for example on the querying of data obtained under Section 702 of the Foreign Intelligence Surveillance Act by the Federal Bureau of Investigation, the implementation of the Board's recommendations on Presidential Policy Directive 28, etc.);

(iii) the reauthorisation of Section 501 of the Foreign Intelligence Surveillance Act, in particular that the existing safeguards remain in place; and
(iv) the evolving U.S. case law on judicial redress in the area of government surveillance, in particular with respect to the issue of standing before the courts.

Regarding the expiring FISA provisions which will end in mid-December absent enacted legislation, the EC remarked "[s]ince the collection under Section 501 of the Foreign Intelligence Surveillance Act is relevant in the context of the Privacy Shield and has therefore been assessed in the Commission adequacy decision, it is important that in case of reauthorization, the existing limitations and safeguards, such as the prohibition of bulk collection, remain in place." Of course, in an August letter sent before he stepped down, former DNI Dan Coats asked the Senate Intelligence and Judiciary Committees for "the permanent reauthorization of the provisions of the USA FREEDOM Act of 2015 that are currently set to expire in December…[that] provide the IC with key national security authorities," including a permanent reauthorization of language allowing for bulk collection of telephony metadata (aka call detail records). It is not clear if this is still the Trump Administration's position, but it would be diametrically opposed to what the EC would like to see.

Regarding PCLOB oversight activities, in July the board said it would be examining a number of U.S. activities of relevance to the EC in the context of Privacy Shield, including the NSA's Collection of Call Detail Records under the USA Freedom Act, Examination of certain counterterrorism-related activities conducted pursuant to Executive Order 12333, and FBI Querying, Compliance, and Information Technology. To date, the PCLOB has not yet released any of the determinations made regarding these topics.

The EC, moreover, noted it "will continue to follow closely the ongoing debate about federal privacy legislation in the U.S." The EC claimed "[a] comprehensive approach to privacy and data protection would increase the convergence between the EU and the U.S. systems and this would strengthen the foundations on which the Privacy Shield framework has been developed." Of course, the EC is likely hinting at a privacy and data protection regime along the lines of the General Data Protection Regulation and related EU directives and may find some of the bills proposed (e.g. the "Information Transparency & Personal Data Control Act" (H.R. 2013), the bill endorsed by the New Democrat Coalition) inadequate.

Of course it must be said that there are two challenges moving through Europe's court systems that may result in part if not all of Privacy Shield being struck down on the basis of U.S. law and practices as the predecessor agreement Safe Harbor was struck down, necessitating the hurried drafting and adoption of the Privacy Shield. Rulings are expected next year, and adverse rulings could necessitate Congressional action as it did before Privacy Shield could move forward. In one of the cases, the Austrian privacy advocate Maximillian Schrems is arguing that Privacy Shield should be struck down in its entirety. Schrem's organization, None of Your Business (NOYB), has provided its summary of the issues before the Court of Justice of the European Union (CJEU):

Core Arguments by the Parties

- The **Irish Data Protection Commissioner** joins Mr. Schrems in his view that US surveillance laws violate fundamental rights to privacy, data protection, and redress under European law. The DPC says, however, that she has no powers to solve the issue. Because the data transfer mechanism Facebook uses (Standard Contractual Clauses) does not foresee such a situation, the clauses themselves need to be invalidated. This would mean that data transfers to any non-EU country under this instrument would have to be stopped.

- **Facebook** takes the view that US law does not go beyond what is legal under EU law. Facebook also questions whether the EU has any jurisdiction on "national security" cases. In summary Facebook sees no problem to continue to transfer data to the United States under mass surveillance laws like FISA. Facebook also relies on the European Commission's assessment of US law in the so-called "Privacy Shield" decision, which says that US surveillance laws comply with EU requirements.
- **Schrems** agrees with the DPC on the problem, but proposes a more measured solution. The law (Article 4 SCCs) permits the DPC to stop individual data transfers (like Facebook's). Mr. Schrems says that the Irish DPC has a duty to act, instead of kicking the case back to the CJEU. On Facebook's reliance on the "Privacy Shield", Mr. Schrems takes the view that the Privacy Shield Decision by the European Commission does not adequately describe US surveillance laws, is not even remotely capable of providing adequate privacy protections, and must therefore be invalidated.
- **European Commission:** The European Commission is expected to defend both its decisions: The Standard Contractual Clauses and Privacy Shield. It will likely side with the United States and Facebook on the view that there is no violation of fundamental rights in the United States, but also acknowledge that the DPC has the power to solve the issue itself if the CJEU sees a violation of fundamental rights in the US.

House Homeland Security Looks At Future Threats

The House Homeland Security Committee's Cybersecurity, Infrastructure Protection, & Innovation Subcommittee held a hearing focused on future cyber threats and heard from the following witnesses:

- Symantec Corporation Senior Strategist Ken Durbin
- Northeastern University Senior Research Scientist and Council on Foreign Relations Senior Fellow Robert Knake
- New America Cybersecurity Initiative Senior Fellow Niloofar Razi Howe
- Georgetown University Assistant Teaching Professor Ben Buchanan

Subcommittee Chair Cedric Richmond (D-LA) said that "[t]he rapid proliferation of new technology is changing the world…[and] [a]dvancements in Artificial Intelligence (AI) and quantum computing will equip us with new tools to defend ourselves and break down barriers to new research that could improve the way we live and save lives." He stated that "[u]nfortunately, one man's tool is another man's weapon…[and] [s]ophisticated nation-state actors like Russia, China, Iran, and North Korea have already weaponized new technologies to disrupt our democracy, compromise our national security, and undermine our economy."

Richmond stated that "[a]s technology improves, so will their ability to use it against us...[and] I am particularly concerned about the impact of new technologies on our elections." He stated that "[i]n the lead up to the 2016 Presidential election, Russia mounted an unprecedented influence and disinformation campaign that used bots to automatically tweet divisive messages from fake accounts." Richmond stated that "[a]s we move into the heart of the 2020 election cycle, we must be prepared for our adversaries to use AI-generated "deep fakes" to create a false history, sow discord, and inject skepticism into our national elections." He asserted that "[t]o start, online platforms must learn to identify "deep fakes" and publish policies about how they will handle them." Richmond remarked that "[a]t the same time, we need to educate the public to ensure that they are informed consumers of information…[and] [m]ore broadly, ensuring that emerging technologies are

developed and deployed responsibly requires U.S. leadership, and I am concerned that we are not demonstrating that now."

Richmond stated that "[f]or years, the Federal government has cut research and development dollars to meet budget caps, and I am worried that countries like China are outpacing our investment." He said that "[o]ur failure to put money into R&D may cost us not only our strategic advantage as the world's leader in technology development, but the global influence that stems from it." He said that "[w]hat is most alarming, however, is the lack of attention that this Administration is giving to this important national security issue." Richmond stated that "[d]espite the fact that our intelligence agencies have confirmed that nation state actors are utilizing the emerging technology for their strategic advantage, the Administration annually slashes R&D funding under the false promise that the private sector will make up the difference." He claimed that "[m]aintaining U.S. leadership in this space will require direction, coordination, and money from the Federal government."

Subcommittee Ranking Member John Katko (R-NY) stated that "[a]s I have learned about the cyber landscape as Ranking Member of this subcommittee, I have been amazed at the number and diversity of the cyber threats we face." He stated that "[t]hese threats are always evolving and adapting to new obstacles, new protections, new tactics, and new technologies…[and] [a]ll levels of government – federal, state and local, as well as, our allies around the globe – the private sector, academia and non-profits must work together in order to protect against emerging cyber threats." Katko stated that "[t]oday's technologies have a number of vulnerabilities that must be protected from bad actors. In the first six months of this year, more than 4 million records have been exposed due to data breaches. Ransomware attacks have doubled in 2019." He asserted that "[c]ybercrime made up 61 percent of the attacks that cybersecurity firm, Crowdstrike, saw between January and June of this year…[a]nd these are just the attacks and statistics that we are aware of; many experts believe incidents to be under-reported."

Katko stated that "[t]hese threats are persistent, complex and on the rise, and cybersecurity must constantly evolve in order to provide protection." He stated that "[a]s evidenced by the number of incidents in this year alone, this is a difficult endeavor that cannot be done without help." Katko stated that "[a]nd these are just the threats we see with our current technology…[and] [o]ur cyber landscape is becoming increasingly sophisticated and new innovations are being introduced every day." Katko stated that "[t]hese advances could put cybersecurity out of reach for even more small, medium and large businesses as well as state and local governments." He said that "[i]t is estimated that 22 million internet of things devices will be online by 2025…[and] 5G deployment is just around the corner."

Katko contended that "[t]hese emerging technologies will undoubtedly present new and evolving cyber threats." He stated that "[w]hile we are staying vigilant and working to protect against current hazards, we must also be preparing for future ones…[and] [o]ur first step is to better understand these new threats and this hearing is a good start."

Committee Chair Bennie Thompson (D-MS) stated that "[w]hen this Committee was established a decade-and-a-half ago, we once focused our efforts on defending against physical attacks committed by terrorists who would readily claim responsibility." He said that "[n]ow, we are faced with cyber threats from state and non-state actors who use cyber tools to carry out attacks in secret, blur attribution, and complicate our ability to impose consequences." Thompson said that "[a]s technology continues to evolve, so too will the tools of our adversaries." He noted that "[l]ast

December, DHS, DOD, the State Department, and the Office of the Director of National Intelligence identified Internet of Things (IoT) devices, Artificial Intelligence (AI), and quantum technologies as emerging, dual-use technologies that pose a threat to our national security."

Thompson declared that "[w]e must prepare ourselves to harness the security, economic, and healthcare benefits of emerging technologies like AI and quantum computing will yield while defending ourselves against adversaries who would use technology against us…[b]ut the government cannot do it alone." He added "[t]he private sector is a critical partner in this effort."

Knake stated

> The good news is that technology trends and new doctrine for cybersecurity have dramatically changed the terrain of cyberspace. Companies at the leading edge of cybersecurity have been able to manage the threat from even the most sophisticated actors. If these trends continue and if policy is put into place to correctly align incentives, it is possible that in five years we may view cybersecurity broadly as a manageable problem. The bad news is that emerging technologies may once again favor the attacker, erasing the defensive gains of the past decade.

Knake said that "[t]oday, I believe we are starting to recognize that markets alone will not solve our cybersecurity dilemma…[and] I think it is fair to conclude that the industries that are doing the best at actively managing risk in cyberspace are also actively regulated: financial services and the defense industrial base." He contended that "[m]any of the approaches to security that are working today were pioneered in these sectors…[and] [d]riving these innovations to other markets will require creating the right set of incentives and requirements." Knake stated that "I have been pleased to see that more so than in any previous Administration, the current leadership of the Department of Homeland Security has recognized that regulation, smartly and carefully implemented, is necessary to drive the level of security required for our nation…[and] [t]he Department's cybersecurity strategy is explicit on this point."

Knake stated that

- In the Internet of Things (IOT) space, DHS should lead efforts to regulate the security of IOT devices in the sectors that it regulates including chemicals, pipelines, and the maritime industry…[and] I believe that the Internet of Things Cybersecurity Improvement Act (S. 734/H.R. 1668) would be a good first step toward improving IOT security. The Act would set standards that sellers of IOT technology to the Federal government would need to meet as well as establish disclosure requirements when manufacturers discover vulnerabilities. The approach uses government's massive purchasing power to improve security more broadly. Companies that develop technologies on a "build once, sell everywhere" model will likely meet the governments requirement for all their commercial offerings rather than just for those sold to government. These requirements, once set, could then be adopted to regulate the use of IOT in critical infrastructure sectors.
- Fundamentally, however, I believe that setting requirements is insufficient. We need to make device makers responsible for the full lifecycle of security by making them liable for harm caused by their devices. I recognize that this notion is a radical departure from how we have approached liability within the information technology realm thus far but now that these devices are making their way into national security systems and life safety systems, I think it is critical that we create incentive structures that truly value security.

- Beyond, IOT, the leadership of the Cybersecurity and Infrastructure Security Agency (CISA) has made election security the agencies number one priority. CISA will need to build on its current efforts to counter-election interference to play a role in combating the proliferation of deepfakes in the political realm and for enterprise security. Crucial to this effort will be building strong, operational partnerships with social media companies that go well beyond today's arm length interactions. Steps must be taken to breakdown the reluctance by Facebook, Google, Twitter, and other social media companies to truly partner with government on this problem.
- For quantum computing and artificial intelligence, government's role should be less about managing the cybersecurity implications and more focused on ensuring that the United States competes and wins in these technologies. I tend to be skeptical of analogies to arms races or calls for Apollo Programs or Manhattan projects, but on the basic science in these fields, those kinds of approaches are warranted. Both China and Russia have made gaining an advantage in AI a national priority. China has also done that on quantum. I believe our market based approach to technology development comes with real advantages but in the development of these core capabilities, I worry that a race that is the Chinese state vs. Silicon Valley is one that Silicon Valley will lose. We need a national effort to ensure that US technology leadership continues into the next decade.

Razi Howe detailed "[a] bold new cyber agenda should include the following elements:

1.Speed and transparency: The US government must remove any barriers that prevent government agencies that have threat and adversary information from sharing that information real-time and with context with the entities that are most affected.

2. A relentless focus on unique value drivers and outcomes.

a. Government's unique role. Government must do what only the government can do—deter malfeasance in cyberspace, especially by nation-state adversaries, by using our tools of national power against those adversaries who are harming us. The private sector cannot defend itself alone against nation-state adversaries and criminals who are agile, persistent and creative. Even the strongest walls will eventually succumb to a capable well-funded adversary if there is no deterrence. This is uniquely the government's role.

b. Private sector's unique expertise. The private sector has developed deep technical expertise in certain domains and the US government must leverage the private sector better and not duplicate effort in areas where private sector capabilities now surpass government capabilities. In the threat intelligence market, while US intelligence agencies can bring the full power of their capabilities to bear on a selected basis producing unique insights into foreign adversaries, the private sector has advanced capabilities across a broad group of actors (foreign and domestic), including insight into attacker behavior, tactics techniques and procedures (TTPs), and campaigns.

3. Resilience to ransomware. Ransomware is no longer just a cybercrime issue. Ransomware at the state and municipal level is a national security and homeland security issue. The single purpose of government is to provide services (including protection) to its citizens. Ransomware at scale keeps that from happening as we saw in Baltimore, Atlanta and the State of Texas. It will take a coordinated effort across the whole of government, but especially DHS CISA, NIST, FBI and NSA's Cybersecurity Directorate, working hand in hand with state and local agencies, to make progress against this real threat and to stay ahead of the adversary.

4. Support secure smart cities. As a corollary to the ransomware issue, Congress should provide more support to sub-federal entities to collaborate on smart city modernization projects. Our cities do not have the expertise to defend themselves on their own nor the resources to do it.

5. Commit to regaining our innovation edge. Government funding of innovation so that the US can regain its edge in next generation technologies will be critical to ensuring that those technologies and the infrastructure that supports them is secure by design. The United States must significantly increase (to the tune of multiple of current federal R&D budgets) its funding in basic and applied research in the areas identified by the U.S. intelligence community such as artificial intelligence, 5G, and quantum computing in order to meet its declared national technology priorities. It is time for the government to fund a bold innovation agenda that will carry us forward to 2030 and beyond, and commit to regaining our innovation edge in these critical next generation technologies.

6. Fund media literacy programs. We live in a polarized, hyperconnected world of impatient digital citizens who are being continuously and creatively targeted with misinformation. Developing and funding a media literacy program that teaches individuals how to discern the difference between fact, opinion, misdirection and lies, is critical to a well-functioning society and should be a homeland security priority.

7. Commit to building a diverse workforce in cybersecurity. The government is in a unique position to contribute and commit to purposefully reducing the skills shortage in the cybersecurity industry. While there are some great programs in place, including DHS' CyberPatriot competition, CyberCorps Scholarship for Service initiative, and the April 2019 Executive Order focused on reskilling and upskilling federal employees, more needs to be done to recruit individuals from outside our typical skill sets (IT, law enforcement and military) with a clear mandate of solving the diversity gap in the industry. The cybersecurity workforce today significantly lags behind the broader technology industry in terms of diversity and to solve our skills shortage we need all of society to be inspired by the mission to reclaim cyberspace for good.

8. Judicious implementation of regulation. Regulation must be pursued in a focused and purposeful manner with a willingness to adjust and adapt as we evolve, as technology evolves and as our adversaries evolve. With those guiding principles, we should enact regulation targeted at very specific areas where we can have measurable impact.

   a. Setting minimum Security Standards for IoT is critical. Congress should enact basic regulation with respect to IoT. The US Government can help protect the 5G ecosystem of billions of connected devices by setting basic security standards, requiring features such as auto update, and importantly providing the right incentives, including tax incentives for vendors to implement these standards and corporations (including critical infrastructure) to deploy secure products and the financial headroom and reason to make changes.

   b. It is time to enact regulations on big data and social platforms. The aim is not to regulate "Big Tech" but rather those technology platforms that facilitate communications and propaganda networks, exploit human weakness for profit, are addictive by design, reward virality, not veracity, thereby enabling destructive and chaotic social manipulation by our adversaries, without providing clear benefits to their users that outweighs these costs. These social platforms have demonstrated an unwillingness to self-regulate or put the interests of their consumers or society at large ahead of their profit motivation. The scope of harm they have caused society includes not only the amplification of polarization, but also psychological harm as

the amount of stress, anxiety and depression caused by their platforms is on the rise in society and especially with our youth. They are out of time.

Senators Want TikTok Investigated As Potential National Security Threat

Senate Minority Leader Chuck Schumer (D-NY) and Senator Tom Cotton (R-AR) have sent their third letter in the last month regarding the threat posed by the operation of a Chinese technology company in the U.S. In this letter, they claim that TikTok poses national security risks to the U.S. and ask "the Intelligence Community conduct an assessment of the national security risks posed by TikTok and other China-based content platforms operating in the U.S. and brief Congress on these findings." As you may recall, Schumer and Cotton sent a letter to the Department of Defense asking whether the Department of Defense (DOD) has been updating a list of "those persons operating directly or indirectly in the United States or any of its territories and possessions that are Communist Chinese military companies" as directed by Section 1237 of the FY 1999 NDAA" and another letter to the Federal Communications Commission (FCC) regarding the agency's "legacy authorizations to Chinese state-owned telecommunications companies operating in the U.S."

In their letter to Acting Director of National Intelligence Joseph Maguire, Schumer and Cotton noted that "TikTok is owned by Beijing-based technology company ByteDance, which operates several other content platforms in China." They asserted that "TikTok's terms of service and privacy policies describe how it collects data from its users and their devices, including user content and communications, IP address, location-related data, device identifiers, cookies, metadata, and other sensitive personal information." Schumer and Cotton stated that "[w]hile the company has stated that TikTok does not operate in China and stores U.S. user data in the U.S., ByteDance is still required to adhere to the laws of China." Specifically, they pointed to "China's vague patchwork of intelligence, national security, and cybersecurity laws [that] compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party." Schumer and Cotton asserted that "[w]ithout an independent judiciary to review requests made by the Chinese government for data or other actions, there is no legal mechanism for Chinese companies to appeal if they disagree with a request." Schumer and Cotton further detailed concerns "regarding the potential for censorship or manipulation of certain content," namely TikTok censoring "materials deemed politically sensitive to the Chinese Communist Party, including content related to the recent Hong Kong protests, as well as references to Tiananmen Square, Tibetan and Taiwanese independence, and the treatment of Uighurs."

Schumer and Cotton lauded the Trump Administration for "rightly taken initial steps to address other critical security risks posed by China" but called for "further action is needed, particularly as China continues to shut out U.S.-based technology firms while promoting and expanding the global reach of its own companies." They argued that "[w]ith over 110 million downloads in the U.S. alone, TikTok is a potential counterintelligence threat we cannot ignore." Consequently, Schumer and Cotton asked "that the Intelligence Community conduct an assessment of the national security risks posed by TikTok and other China-based content platforms operating in the U.S. and brief Congress on these findings."

Schumer and Cotton appear intent on keeping the spotlight on Chinese technology companies and the threats they allegedly present to U.S. national security. It seems likely they will continue to press the Trump Administration to investigate and take action against some of these companies.

In response, TikTok claimed that all its data is stored in the U.S. with additional capacity in Singapore, thus putting all its data beyond the reach of the Chinese government. TikTok further asserted "[o]ur U.S. moderation team, which is led out of California, reviews content for adherence to our US policies – just like other US companies in our space." The company stated that "[w]e are not influenced by any foreign government, including the Chinese government; TikTok does not operate in China, nor do we have any intention of doing so in the future." ByteDance operates a similar but different app in China called Douyin, which presumably could be operated to meet Chinese law without bearing on how TikTok is operated in the U.S.

TikTok's statement seems to also encompass a different Senator's request that the social media platform be investigated. Earlier this month, Senator Marco Rubio (R-FL) asked the Secretary of the Treasury Steven Mnuchin requesting that the Committee on Foreign Investment in the United States (CFIUS) conduct "a full review of the national security implications of TikTok's acquisition of Musical.ly." Rubio stated

> According to reports, TikTok acquired Musical.ly, a video-sharing platform, without any oversight and relaunched the service for Western markets. These Chinese-owned apps are increasingly being used to censor content and silence open discussion on topics deemed sensitive by the Chinese Government and Communist Party. These topics include Tiananmen Square, Tibet, Hong Kong, Taiwan, and other issues.

Rubio commended CFIUS "for its recent work in this space against Beijing Kunlun Tech Co Ltd, which took majority ownership of [Grindr] that contained user's personal and sensitive data…[and] [w]ithout intervention, there is no saying how this information would have been used by the Chinese government."

If CFIUS should launch an investigation of TikTok, it would be the second federal probe this year. In February, the Federal Trade Commission (FTC) announced the then largest settlement with TikTok under the Children's Online Privacy Protection Act (COPPA). The agency argued that "that the operators of the Musical.ly app violated the COPPA Rule by failing to notify parents about the app's collection and use of personal information from users under 13, obtain parental consent before such collection and use, and delete personal information at the request of parents.

Specifically, the FTC alleged and TikTok agreed:

> [Music.ly] violated the COPPA Rule and the FTC Act by failing to post a privacy policy on its online service providing clear, understandable, and complete notice of its information practices; failing to provide direct notice of its information practices to parents; failing to obtain verifiable parental consent prior to collecting, using, and/or disclosing personal information from children; failing to delete personal information at the request of parents; and retaining personal information longer than reasonably necessary to fulfill the purpose for which the information was collected.

Memorandum Alleges Deliberate Forcing Out of Senior White House Cyber Staff; Congressman Presses For Answers

Last week, *Axios* published an article based on a memorandum submitted by former White House Computer Network Defense Branch Chief Dimitrios Vastakis along with his resignation that predicted current White House cybersecurity priorities will inevitably result in another breach along the lines

of a Russian breach of unclassified White House systems in 2014. Anonymous White House sources bolstered Vastakis' claims that a planned reorganization of how the White House secures itself and networks from hackers could make such an event more likely. It was also alleged that the staff being forced out are Obama Administration appointees. To date, the White House has not commented officially on the report or the memorandum.

Vastakis decried the absorption of the Office of the Chief Information Security Officer (OCISO) into the Office of the Chief Information Officer (OCIO), which he characterized as "a significant shift in the priorities of senior leadership where business operations and quality of services take precedence over securing the President's network." In July, the White reportedly reorganized OCISO into OCIO, and in August former White House CISO Joe Schatz left. He added that "[a]lso of concern is the metric leadership is leveraging to gauge success of the cybersecurity program." Vastakis contended that "[m]easuring the success of your security staff by the frequency major compromises are identified versus the duration since the last compromise is absurd." He stated his "express opinion that the remaining incumbent OCISO staff is systematically being targeted for removal from the Office of Administration (OA) through various means, such as: revocation of incentives; reducing the scope of duties; reducing access to programs; revoking access to buildings; and revoking positions with strategic and tactical decision making authorities." He claimed that "being habitually hostile to incumbent OCISO staff…a staple tactic for the new leadership…has forced the majority of GS-15 and GS-15 OCISO staff to resign."

Vastakis said "I have seen the planned organizational structure for the cybersecurity mission going forward [that]…essentially transfers the entire mission to the White House Communications Agency (WHCA)." He argued that "[a]ll key decision making roles and leadership positions will no longer be staffed by Executive Office of the President (EOP) individuals." Vastakis asserted that "given all the changes I've seen in the last three months, I foresee the White House is posturing itself to be electronically compromised once again," referring to the aforementioned 2014 hack reported in the popular media.

Following the *Axios* article, Representative Ted Lieu (D-CA) wrote acting White House Chief of Staff Mick Mulvaney "with great concern about recent reports suggesting that at least 12 senior White House cybersecurity officials have left or been forced out of their roles, potentially weakening the White House's network defense." Lieu stated that "[w]hile the immediate concern of a potential network breach is paramount, cyber infiltration can also result in a long term serious threat to national security." He added that "the apparent effort to move cybersecurity operations into an office exempt from the Presidential Records Act fits the President's history of obstructing and hiding transcripts and government business by manipulating internal bureaucratic procedures." Lieu argued that "[a] White House data breach would give our adversaries an untold advantage in almost every foreign policy and national security matter…[and] [t]herefore, I request answers to the following questions:

- Is your office aware of efforts by members of the President's team to oust career cybersecurity officials without good cause?
- Are you taking immediate steps to staff the OCISO with qualified replacements following the mass departure of career employees, as detailed in the aforementioned article?
- Why have White House cybersecurity responsibilities been delegated to the Office of the Chief Information Officer (OCIO), which is not covered under the Presidential Records Act?
- Will you commit to providing Congress with documents related to the decision to collapse OCISO into the OCIO?

- Have you been in contact with intelligence agencies including the Office of the Director of National Intelligence and the National Security Agency about the concerns raised in Mr. Vastakis' memo?

Senators Ask FTC To Investigate Amazon's Role In The Capital One Breach

This week, Senators Elizabeth Warren (D-MA) and Ron Wyden (D-OR) requested that the Federal Trade Commission (FTC) "to open an investigation to determine if Amazon's failure to secure the servers it rented to Capital One may have violated federal law" in light of the breach announced by Capital One in late July that may affect as many as 100 million Americans. The Senators claimed that Amazon has failed to institute measures to protect against server-side request forgery (SSRF) attacks unlike its competitors. The Warren/Wyden letter follows an August exchange between Wyden and the company regarding this breach. They called on the FTC to investigate this failure and determine whether it qualifies as an unfair practice that violates Section 5 of the FTC Act.

Warren and Wyden noted that "SSRF attacks can be used by hackers to steal valuable data from servers rented from cloud computing companies…[and] Amazon's largest competitors have included mandatory protections against SSRF attacks in their products for several years — Google since 2013 and Microsoft since 2017." They claimed that "Amazon's failure to add a similar software protection against SSRF attacks to its Amazon Web Services (AWS) cloud computing product has been the subject of significant public discussion among cybersecurity experts for the past five years, including in presentations at major industry conferences."

Warren and Wyden stated "the FTC has made it clear that companies have an obligation to act on third-party reports of cybersecurity vulnerabilities" and cited the 2013 FTC action HTC, in which the agency "established that companies must "implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public." Warren and Wyden noted that "HTC's failure to do so, the FTC argued then, constituted an unfair business practice."

Warren and Wyden stated that "[w]hile it is likely that Amazon has known that its AWS product was vulnerable to SSRF attacks since the first high-profile demonstration by a cybersecurity researcher in 2014, the company has certainly known since mid-2018 at the latest." They asserted that "[i]n August of 2018, Amazon's security team was contacted by email by a cybersecurity expert, who recommended that Amazon adopt the same cybersecurity defense against SSRF attacks already used by Google and Microsoft" and provided a redacted copy of the email. Warren and Wyden claim "Amazon knew, or should have known, that AWS was vulnerable to SSRF attacks…[and yet AWS] continues to sell defective cloud computing services to businesses, government agencies, and to the general public." They contended that "[a]s such, Amazon shares some responsibility for the theft of data on 100 million Capital One customers."

Wyden wrote Amazon in August "to better understand how default configuration settings for Amazon's cloud computing products may have contributed to recent data breaches of servers used by Capital One Financial Corporation (Capital One) and several other large organizations." Wyden posed a number of questions to Amazon based on the view of "[a] number of cybersecurity experts [that] have publicly speculated that the Capital One hacker exploited a SSRF vulnerability." In their response, Amazon claimed:

> As Capital One outlined in their public announcement, the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended. After gaining access through the misconfigured firewall and having broader permissions to access resources, we believe a SSRF attack was used (which is one of several ways an attacker could have potentially gotten access to data once they got in through the misconfigured firewall).

However, Wyden had released neither his letter nor Amazon's response until he and Warren sent their letter.

In a likely unrelated development, the Department of Defense (DOD) announced that it had selected Microsoft over AWS for its $10 billion cloud contract. The Joint Enterprise Defense Infrastructure (JEDI) bidding process has been fraught with litigation alleging unfair influence on the part of AWS given its hiring of a Pentagon official who was working on the JEDI procurement and reports that President Donald Trump told the DOD not to award the contract to Amazon, which also owns *The Washington Post,* an entity with which Trump has often clashed. In its statement, the DOD characterized the award as a continuation of "our strategy of a multi-vendor, multi-cloud environment as the department's needs are diverse and cannot be met by any single supplier." The Pentagon noted that it has awarded "more than $11 billion across 10 separate cloud contracts" as part of its DOD Cloud Strategy.

FTC Acts Against Stalking App

The Federal Trade Commission (FTC) announced its first action the developer of applications for smart phones that may be placed on a user's device without their knowledge or consent (aka stalking apps). The FTC took action against the developer of stalking apps of violating both the Federal Trade Commission Act (FTC Act) and the Children's Privacy Protection Rule (COPPA Rule). In its press release, the FTC claimed these apps "allowed purchasers to monitor the mobile devices on which they were installed, without the knowledge or permission of the device's user."

Retina-X Studios, LLC agreed to a consent order that permanently restrains and enjoins the company "from, or assisting others in, promoting, selling, or distributing a Monitoring Product or Service unless Respondents" meet a list of requirements, including foreswearing the circumvention of a mobile device's operating system for installation (aka jail-breaking or rooting), eliciting affirmative agreement that users of any such app will only employ it in lawful, enumerated practices, and that whenever the app is running, there must be a clear and conspicuous icon on the device alerting the user that the run has been installed and is functional.

The FTC explained that Retina-X offered three apps:

a. MobileSpy: Respondents' MobileSpy mobile device monitoring product and service ("MobileSpy") was marketed as a product to monitor children or employees. MobileSpy first became available in 2007, and Respondents sold more than 5,700 MobileSpy licenses. Once installed, MobileSpy captured and logged, among other things, the following: text messages; messages sent and received on various messaging services; call history; keys pressed; GPS locations; photos; contact list; screenshots; and browser history. MobileSpy's premium version also permitted monitoring consumers, from a remote online dashboard, to view the monitored mobile device's screen in real time.

b. PhoneSheriff: Respondents' PhoneSheriff mobile device monitoring product and service ("PhoneSheriff") was marketed as a product to monitor children. PhoneSheriff first became available in 2011, and Respondents sold more than 4,600 PhoneSheriff licenses. Once installed, PhoneSheriff captured and logged, among other things, the following: GPS locations; text messages; messages sent and received on various messaging services; call history; photos; contact list; browser history; notes; music files; calendar entries; applications installed; mobile usage summaries; email history; and screenshots of any activity using the Snapchat application.
c. TeenShield: Respondents' TeenShield mobile device monitoring product and service ("TeenShield") was marketed as a product to monitor children. TeenShield first became available in 2015, and Respondents sold more than 5,000 TeenShield licenses. As part of the TeenShield for iOS registration process, Respondents collected dates of birth of users being monitored. From February 2016 to October 2017, Respondents collected approximately 950 dates of birth, and about a third of those were for children under the age of 13. Once installed, TeenShield captured and logged, among other things, the following: GPS locations; text messages; messages sent and received on various messaging services; call history; photos; contact list; browser history; and email history.

The FTC noted "[p]urchasers were often required to jailbreak or root (i.e., actions to bypass various restrictions implemented by the operating system on and/or the manufacturer of mobile devices) the device user's mobile device prior to installing Respondents' monitoring products and services." The agency stated "[j]ailbreaking or rooting a mobile device can expose a mobile device to various security vulnerabilities and likely invalidates any warranty that a mobile device manufacturer or carrier provides."

The FTC stated that "[r]espondents' monitoring products and services substantially injured device users by enabling purchasers to surreptitiously stalk them…[and] [s]talkers and abusers use mobile device monitoring software to obtain victims' sensitive personal information without authorization and surreptitiously monitor victims' physical movements and online activities." The FTC alleged the following injuries:

- [V]ictims of stalking experience financial loss both directly and indirectly. Directly, stalkers and abusers can use the information obtained through monitoring products and services to take over a victim's financial accounts, and redirect any (or all) funds to the abuser. Furthermore, victims suffer financial loss in the form of lost warranty coverage resulting from jailbreaking/rooting a mobile device and the purchase of a new mobile device to ensure that they are no longer subject to surreptitious monitoring. Indirectly, victims experience financial loss through the costs associated with therapy or counseling, and moving away from an abuser.
- The sale of Respondents' surreptitious monitoring products and services also substantially injured device users by undermining the mobile device security features provided by their operating system or manufacturer.

The FTC concluded that "[t]hese harms were not reasonably avoidable by consumers, as users had no way to know that their mobile devices were being surreptitiously tracked using Respondents' monitoring products and services…[and] are not outweighed by countervailing benefits to consumers or competition."

The FTC further alleged that Retina-X Studios failed to implement and maintain proper data security practices despite claiming: "[i]t is company policy that our customer databases remain confidential and private...Your private information is safe with us." The agency asserted that:

> Even assuming Respondents believed that their monitoring products and services were being used for legitimate purposes, including the monitoring of children and employees, Respondents did not take steps to secure the personal information collected from purchasers and device users being monitored. As a result, the personal information collected from purchasers and device users was at risk of unauthorized disclosure and use.

The FTC contended that:

> Respondents engaged in a number of practices that, taken together, failed to provide reasonable data security to protect the personal information collected from consumers. Among other things, Respondents failed to:
>
> a. Adopt, implement, or maintain written information security standards, policies, procedures or practices;
> b. Conduct security testing of mobile applications that could be exploited to gain unauthorized access to consumers' sensitive personal information for well-known and reasonably foreseeable vulnerabilities;
> c. Contractually require their service providers to adopt and implement information security standards, policies, procedures or practices;
> d. Perform adequate oversight of service providers; and
> e. Adopt and implement written information security standards, policies, procedures, or practices that would apply to the oversight of their service providers.

The FTC detailed Retina-X Studio's COPPA violations:

- Respondents collected personal information from children under the age of 13 through the TeenShield product, which Respondents operated and had actual knowledge that children were being monitored using these online services.
- In numerous instances, in connection with the acts and practices described above, Respondents collected, used, and/or disclosed personal information from children in violation of the Rule, including by failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children…

The FTC is requiring Retina-X Studios to

- Meet the requirements of the COPPA rule
- Stop misrepresenting how they actually safeguard personal information
- Delete all the personal information collected from the three apps
- Implement a comprehensive data security program
- Pay for an initial and then biennial data assessments from a third-party assessor
- Submit annual certifications by a senior corporate official that the company is meeting the requirements of the settlement, and if not, there must be explanation of any such violations
- Alert the FTC within 10 days after personal data has been accessed or acquired without authorization

Further Reading

- "Russian operatives sacrifice followers to stay under cover on Facebook" – *Reuters*. Facebooks is using the tactics Russian hackers have used to spread disinformation against them. In order to sow discord, the Internet Research Agency's (IRA) hackers need to be outrageous and memorable but doing so makes it easier for Facebook's security team to track and take down these profiles. With the IRA changing techniques, their hackers may prove less effective.
- "Google Accused of Creating Spy Tool to Squelch Worker Dissent" – *Bloomberg*. Depending on your perspective within Google, a new Chrome extension that reports any large calendar events is either a means by which Google executives can monitor and squelch union organizing or is merely a means by which Google employees will not have their calendars jammed with events.
- "U.S. Government Still Uses Suspect Chinese Cameras" – *The Wall Street Journal*. Despite bans on the purchase of Huawei, ZTE, and other Chinese products and services that went into effect in August, one security firm is reporting that thousands of Chinese-made cameras are still in use at federal military and civilian facilities, raising questions about the effect of such a prospective ban and how U.S. agencies are to manage existing Chinese-built information technology currently in use.
- "House antitrust probe report likely by 'first part' of 2020" – *Reuters*. The House subcommittee chair running the investigation into the anti-competitive practices in digital markets envisions releasing their report early next year, likely in time for the Department of Justice, the Federal Trade Commission, and numerous state attorneys general to use in the various anti-trust investigations into a number of large technology companies.
- "Online Influencers Tell You What to Buy, Advertisers Wonder Who's Listening" – *The Wall Street Journal*. The market for advertising in the form of paid but not necessarily transparent celebrity endorsement of products has begun to dip. Some early adopters are now questioning the value of paying someone with thousands or millions of followers to include content in their feed considering saturation in the marketplace and consumers generally be wiser to and warier of such endorsements.
- "Attorney General's Antitrust Power Play Is Just What Trump Wants" – *Bloomberg BusinessWeek*. William Barr is uniquely versed in anti-trust policy, having served as Verizon's general counsel from 1994 through 2008 and was a participant in the battles over the power of telephone and cable companies and net neutrality. His move to have the Department of Justice investigate the same tech companies the Federal Trade Commission is drew criticism inside Washington but may prove favorable to his boss, President Donald Trump.
- "Facebook takedowns show new Russian activity targeted Biden, praised Trump" – *The Washington Post*. The social media giant took down four disinformation campaigns from Instagram, one Russian, and the other three Iranian, seeking to influence the 2020 election. A number of the disinformation efforts sought o widen schisms in the Democratic party among a number of nominees with a particular focus on former Vice President Joe Biden. The Russian efforts are most likely allied with Russia's Internet Research Agency, the entity responsible for the disinformation sown during the last presidential election. The takedowns occurred two days before Zuckerberg appeared before the House Financial Services Committee.
- "Cops Need a Warrant to Access Your Car's Data, Court Rules" – *Vice*. The Georgia Supreme Court reverses two lower courts in finding that the Four Amendment bars warrantless searches of cars for the data they contain. In this case, after a car crash, a police officer downloaded the data from the airbag sensors and learned that one of the people involved was driving at twice the speed limit. The court turned aside all the state's arguments about how this should fit into a number of Fourth Amendment exceptions allowing

what would otherwise be unreasonable searches. It remains to be seen how the U.S. Supreme Court would rule on this issue, especially since Justice Anthony Kennedy was the swing vote in the 2018 case that found warrantless searches of cell phone records a violation of the Fourth Amendment.