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

Spotlight: A Privacy Bill A Week

Key Points:

- *This is the last of the major privacy bills that have been released*
- *The DATA Privacy Act is not as consumer-friendly as the Privacy Bill of Rights but is still much more robust than many of the other bills*

Last week, we spent a bit of time looking at the "Privacy Bill of Rights Act" (S. 1214), the only bill to get an A in the Electronic Privacy Information Center's report on privacy bills, and likely outside the realm of the politically possible at present. This week, we will examine Senator Catherine Cortez Masto's (D-NV) "Digital Accountability and Transparency to Advance Privacy Act" (DATA Privacy Act) (S. 583). Of course, Cortez Masto served as the attorney general of Nevada for eight years prior to succeeding former Senator Harry Reid (D-NV), and this bill demonstrates her background as her state's top prosecutor.

In terms of similarities to the other privacy bills, the Federal Trade Commission (FTC) would promulgate extensive regulations to effectuate a new federal privacy regime under the Administrative Procedure Act (APA) and would be able to punish privacy violations by seeking civil penalties in the first instance in a court action. Consumers would receive the right to opt-in and opt-out of certain data collection, processing, use, sharing, and selling practices conducted by entities.

State attorneys general would be able to bring actions under the new enforcement structure. Consumers would not be allowed to sue for violations of the new regime, which is aligned with a number of other bills.

Like the "Privacy Bill of Rights" (S. 1214), the DATA Privacy Act would rule out of bounds certain practices instead of going the route on enhanced notice and consent like many of the other bills do (i.e. once a consumer is informed of how an entity proposes to collect and use their data, almost any subsequent processing and use would be acceptable.)

In terms of the scope of the DATA Privacy Act, like the "Privacy Bill of Rights Act" (S. 1214), virtually all entities collecting, using and disclosing consumer information would be considered a "covered entity." However, there would be an exception exempting entities that "collect[], process[], store[], or disclose[] covered data relating to fewer than 3,000 individuals and devices during any 12-month period." "Covered data" is "any information that is—

- collected, processed, stored, or disclosed by a covered entity;
- collected over the internet or other digital network; and
- linked to an individual or device associated with an individual; or
- practicably linkable to an individual or device associated with an individual, including by combination with separate information, by the covered entity or any potential recipient of the data."

This definition encompasses much of the current data ecosystem. Any information vacuumed up electronically that is or can be linked to a person or her device would be covered under the bill. However, employment data and government records made available to the public are not covered data.

The bill defines "privacy risk" to be the "potential harm to an individual resulting from the collection, processing, storage, or disclosure of covered data, including—

(A) direct or indirect financial loss;
(B) stigmatization or reputational harm;
(C) anxiety, embarrassment, fear, and other severe emotional trauma;
(D) loss of economic opportunity; or
(E) physical harm."

If enacted, the FTC and courts may have difficulty in determining what exactly constitutes things like "stigmatization or reputational harm," "anxiety, embarrassment, fear, and other severe emotional trauma," or "loss of economic opportunity." What turns out to be a "privacy risk" would likely be shaped on a case-by-case basis after FTC regulations speak to these concepts. Nonetheless, the DATA Privacy Act is one of the few bills that seeks to make what some might consider non-economic or non-tangible privacy injuries illegal conduct.

In terms of the personal information upon which consumers would gain new rights and protections, this bill introduced some new ways of looking at this concept, notably, the following terms:

- A "protected characteristic" is an "individual's race, sex, gender, sexual orientation, nationality, religious belief, or political affiliation."
- "pseudonymous data" are "covered data that may only be linked to the identity of an individual or the identity of a device associated with an individual if combined with separate information."
- a "reasonable interest" means—
    - a compelling business, operational, administrative, legal, or educational justification for the collection, processing, storage, or disclosure of covered data exists;
    - the use of covered data is within the context of the relationship between the covered entity and the individual linked to the covered data; and
    - the interest does not subject the individual to an unreasonable privacy risk.
- "sensitive data" are "any covered data relating to—
    - the health, biologic, physiologic, biometric, sexual life, or genetic information of an individual; or
    - the precise geolocation information of a device associated with an individual.

The FTC is given explicit authority to modify two of these definitions through the rulemaking authority granted the agency (i.e. "pseudonymous data" and "sensitive data"), suggesting the other definitions may not be changed.

Covered entities would need to "post in an accessible location a notice that is concise, in context, in easily understandable language, accurate, clear, timely, updated, uses visualizations where appropriate, conspicuous, and free of charge regarding the covered entity's privacy practices." This notice must inform consumers of "the methods necessary to exercise their rights" described elsewhere in the bill.

Within one year of enactment, the FTC must promulgate regulations that require covered entities "to implement, practice, and maintain certain data procedures and processes" subject to standards that are distinguishable from other privacy bills.

"[R]egarding the means by and purposes for which covered data is collected, processed, stored, and disclosed," covered entities must engage in the following practices to detailed by FTC regulation:

- A covered entity's collection, processing, storage, and disclosure of covered data must be in service of a reasonable interest of the covered entity, such as
    - business, educational, and administrative operations that are relevant and appropriate to the context of the relationship between the covered entity and the individual linked to the covered data;
    - relevant and appropriate product and service development and enhancement;
    - preventing and detecting abuse, fraud, and other criminal activity;
    - reasonable communications and marketing practices that follow best practices, rules, and ethical standards;
    - engaging in scientific, medical, or statistical research that follows commonly accepted ethical standards; or
    - any other purpose for which the Commission considers to be reasonable.

A few observations about a "reasonable interest." First, the FTC can add to this this list, so it is not exhaustive, but those activities not listed here would be deemed unreasonable and therefore not allowed. For example, what might be considered unreasonable "communications and marketing practices"? Advertising by third parties unrelated to the consumer based on the information the covered entity gave or sold the third party? Presumably should this not expose a consumer to a "privacy risk," then it may be permissible. Second, the FTC will need to define a reasonableness standard by which a "business" operation "relevant and appropriate to the context of the relationship between the covered entity and the individual linked to the covered data" may be determined acceptable under the bill. If a consumer is perusing Amazon's website for books on substance abuse addiction and has granted the necessary permissions for the website to use such covered data to sell advertisements on its website aimed at this consumer regarding 12-step programs? Possibly not since this would be "sensitive information" that is protected at a different standard that "covered data."

The bill introduces an equitable standard that would bar the collection, use, disclosure, or processing of covered data in a way that result in discrimination on the basis of a protected characteristic. Consequently, discriminatory targeted advertising practices, "price, service, or employment opportunity discrimination," or any other practice the FTC thinks would result in discrimination on the basis of a protected characteristic would be disallowed. Incidentally, this standard would seem to place the FTC or state attorney general's calculus on what constitutes discrimination on the disparate impact side of the issue as opposed to disparate treatment which usually requires an intent to discriminate. Consequently, Republican and industry stakeholders would likely object to these provisions.

Finally, a forthrightness standard would bar covered entities from a number of potentially deceptive practices, including using "inconspicuous recording or tracking devices and methods," disclosing the contents of a private communication, methods of representations that are misleading, and anything else the FTC decides does not meet this standard.

But, then would not these practices also run afoul of Section 5 of the FTC Act; however, the FTC would not be able to ask a court for fines on the basis of Section 5 violations.

The DATA Privacy Act employs both opt-out and opt-in rights for consumers depending on the type of information in question. Consumers would be able to opt-out of collection, usage, processing, and disclosing "covered data linked to the individual." However, the definition of "covered data" includes data that is both linked to an individual and information that can be reasonably be linked to an individual. This statement of the right to opt-out may be a bit muddled and in need of clarification. Is it all covered data or just the covered data that can be linked to a person?

And yet, consumers would need to express "affirmative, opt-in consent" in a number of situations:

> before the covered entity collects or discloses sensitive data linked to the individual; or
> before the covered entity collects, processes, stores, or discloses data for purposes which are outside the context of the relationship of the covered entity with the individual linked to the data, including—
>> the use of covered data beyond what is necessary to provide, improve, or market a good or service that the individual requests;
>> the processing or disclosure of covered data differs in material ways from the purposes described in the privacy policy that was in effect when the data was collected; and
>> any other purpose that Commission considers outside of context.

Again, the FTC would be given power to further define what data collection, usage, processing, or disclosure practices would require affirmative, opt-in consent. However, opt-in consent would allow covered entities to utilize a consumer's data in many ways. Of course, a question lurking beneath all these enhanced notice and consent regimes is does a consumer's consent make all data usage kosher?

Finally, covered entities would have the responsibility to minimize data including taking "reasonable measures to limit the collection, processing, storage, and disclosure of covered data to the amount that is necessary to carry out the purposes for which the data is collected; and…[storing] covered data only as long as is reasonably necessary to carry out the purposes for which the data was collected."

However, the bill details circumstances under covered entities may dispense with the requirements relating to data security: if the limitations on the collection, processing, storage, or disclosure of covered data would—

- inhibit detection or prevention of a security risk or incident;
- risk the health, safety, or property of the covered entity or individual; or
- prevent compliance with an applicable law (including regulations) or legal process.

The FTC's regulations would also need to include requirements on how covered entities must allow consumers to access, correct, delete, and obtain a portable version of covered data. However, "[i]f the covered data that an individual has requested processed…is pseudonymous data, a covered entity may decline the request if processing the request is not technically feasible." And, this type of data are "covered data that may only be linked to the identity of an individual or the identity of a device associated with an individual if combined with separate information." Moreover, a covered entity may not retaliate or discriminate against a consumer that avails herself of these

rights by "denying goods or services to the individual;" "charging, or advertising, different prices or rates for goods or services;" or "providing different quality of goods or services."

The DATA Privacy Act links privacy and data security legislation, a feature favored by Democrats more than Republicans. The FTC's regulations would "require covered entities to establish and implement policies and procedures regarding information security practices for the treatment and protection of covered data." Among the elements these new regulations must address "the level of identifiability of the covered data and the associated privacy risk…[and] the sensitivity of the covered data collected, processed, and stored and the associated privacy risk." The FTC must also consider current "technological, administrative, and physical" safeguards, the costs of a covered entity implementing and maintaining and regularly reviewing safeguards. Finally, the FTC is required to weigh how regulations would affect small and medium-sized businesses.

As mentioned both the FTC and state attorneys general could enforce the new regime, and the FTC could intervene in any state action.

Senate and House Move Narrow Cyber Bills; Committees Consider Other Bills

Key Points:

- *With the end of both the calendar and legislative years rapidly approaching, Congress considered a range of cyber-related bills*

In the last week before a two-week recess, both chambers of Congress passed bills without recorded votes that would address targeted aspects of cybersecurity.

the Senate took up, amended, and passed a House bill that, broadly speaking, would codify the Department of Homeland Security's (DHS) cyber hunt and response teams that assist entities in need of cyber-response help. The "DHS Cyber Hunt and Incident Response Teams Act of 2019" was passed by unanimous consent on September 24. DHS's enabling statute would be amended to require the Cybersecurity and Infrastructure Security Agency's (CISA) National Cybersecurity and Communications Integration Center (NCCIC) to

> maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request

NCCIC would also "define the goals and desired outcomes for each cyber hunt and incident response team" and then develop metrics to gauge how well these teams are performing.

In June, the House took up and passed the "DHS Cyber Incident Response Teams Act of 2019" (H.R. 1158), as amended, by voice vote. This version of H.R. 1158 would require NCCIC to "maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

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

- Such other capabilities as the Under Secretary…determines appropriate."

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

The House also passed cybersecurity-related bills by voice vote this week:

- The "Cybersecurity Vulnerability Remediation Act" (H.R. 3710) "seeks to improve how the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) helps Federal and non-Federal entities manage known cybersecurity risks" according to the committee report. This bill "would authorize the CISA Director to identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities--including for software or hardware that is no longer supported by the vendor…[and] would authorize the DHS Under Secretary for Science and Technology to establish an incentive-based program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities."
- The "Unifying DHS Intelligence Enterprise Act" (H.R. 2589) "seeks to improve the Department of Homeland Security's (DHS) intelligence enterprise by ensuring intelligence officers across DHS are sharing information and countering threats in a unified manner" according to the committee report. The bill also "directs the DHS Secretary, acting through the Chief Intelligence Officer, in coordination with intelligence components of the Department, the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, to develop and disseminate written Department-wide guidance for the processing, analysis, production, and dissemination of homeland security information and terrorism information." Finally, H.R. 2589 "requires an assessment and description of how the dissemination to the intelligence community and Federal law enforcement of such information assists such entities in carrying out their respective missions."

On September 25, the House Homeland Security Committee held a markup and approved two bills, one of which was cybersecurity-related:

- The "Cybersecurity Advisory Committee Authorization Act of 2019" (H.R. 1975) introduced by Representative John Katko (R-NY).

The Committee favorably reported H.R. 1975 with an amendment, en bloc, by unanimous consent.

The Committee did not take up the "National Commission on Online Platforms and Homeland Security Act," which had been previously announced for the markup.

H.R. 1975 would establish a Cybersecurity Advisory Committee inside the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) to "advise, consult with, report to, and make recommendations to the Director of CISA on the development, refinement, and implementation of policies, programs, rulemakings, planning, training, and security directives pertaining to the mission of the CISA. Within six months of enactment the CISA Director would name the 35 members of this committee that "shall include representatives of State and local governments and of a broad range of industries." As noted, an amendment was added to expand the universe of representatives CISA must name to the committee to include "the cybersecurity research community, and privacy organizations with expertise and experience."

Moreover, CISA and this new committee are required to "establish subcommittees…to address cybersecurity issues, including relating to the following:

(A) Information exchange.
(B) Critical infrastructure.
(C) Risk management.
(D) Public and private partnerships.

Last week, the House Energy & Commerce Committee's Communications and Technology Subcommittee held a hearing titled "Legislating to Secure America's Wireless Future," at which it discussed a number of bills that would address supply chain issues in U.S. telecommunications networks. The hearing and the bills show Congress' continued focus on information and communications technology sourced from the People's Republic of China. The committee's staff memorandum explained:

> Given the pivotal role that private communications networks serve in connecting U.S . critical infrastructure functions, American networks are appealing targets for foreign adversaries. The United States, therefore, has a clear interest in mitigating threats posed by vulnerable communications equipment and services. In particular, the United States identified individual Chinese telecommunications firms, including Huawei Technologies Co. Ltd (Huawei) and its affiliates, as posing significant threats to U.S . commercial and security interests.

The Subcommittee discussed the following bills as explained in the staff memorandum:

- The "Secure and Trusted Communications Networks Act" (H.R. 4459) instructs the FCC to develop and maintain a list of communications equipment and services that pose an unacceptable risk to national security and prohibits the use of Federal funds to purchase, rent, lease, or otherwise obtain such equipment and services. The bill also establishes the Secure and Trusted Communications Reimbursement Program to assist communications providers with the costs of removing prohibited equipment and services from their networks and replacing prohibited equipment with more secure communications equipment and services.
- The "Network Security Information Sharing Act" (H.R. 4461) directs the Secretary of Homeland Security, in cooperation with the Director of National Intelligence (DNI), the Director of the Federal Bureau of Investigation, NTIA, and FCC, to establish a program to share supply chain security risks with advanced communications service providers and trusted suppliers of telecommunications equipment and services.
- The "Secure 5G and Beyond Act" (H.R. 2881) directs the President to develop the "Secure Next Generation Mobile Communications Strategy" in consultation with the heads of the FCC, NTIA, and Department of Homeland Security, as well as the DNI and Secretary of Defense. The Secure Next Generation Mobile Communications Strategy is intended to: (1) ensure the security of 5G communications systems and infrastructure in the United States; (2) assist mutual defense allies and strategic partners in maximizing the security of 5G networks and infrastructure in their countries; and (3) protect the competitiveness of U.S . companies, the privacy of American consumers, and the integrity of standards-setting bodies against political influence.
- The "Promoting United States Wireless Leadership Act" (H.R. 4500) directs NTIA to encourage participation by trusted American companies and other stakeholders in standards-setting bodies, and to offer technical assistance to such stakeholder that do elect to participate, in the course of developing standards for 5G networks and future generations of communications networks.

- H. Res. 575 expresses the sense of the House of Representatives that stakeholders involved in the deployment of 5G communications infrastructure should consider adherence to the international security recommendations adopted at the Prague 5G Security Conference in May 2019, known as "The Prague Proposals." The resolution also encourages the President and Federal agencies to promote trade and security policies on the international stage that are consistent with "The Prague Proposals."

On September 25, the Senate Energy & Natural Resources Committee marked up a number of bills, including legislation aimed at shoring up the cybersecurity of the U.S. energy system:

- The "Enhancing Grid Security through Public-Private Partnerships Act" (S. 2095) would require that the Department of Energy "in consultation with State regulatory authorities, industry stakeholders, the Electric Reliability Organization, and any other Federal agencies that the Secretary determines to be appropriate, shall carry out a program—
  (1) to develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities;
  (2) to assist with threat assessment and cybersecurity training for electric utilities;
  (3) to provide technical assistance for electric utilities subject to the program;
  (4) to provide training to electric utilities to address and mitigate cybersecurity supply chain management risks;
  (5) to advance the cybersecurity of third-party vendors in partnerships with electric utilities; and
  (6) to increase opportunities for sharing best practices and data collection within the electric sector.
- The "Energy Cybersecurity Act of 2019" (S. 2333) would require the Department of Energy "in consultation with appropriate Federal agencies, the energy sector, the States, and other stakeholders, shall carry out a program—
  (A) to develop advanced cybersecurity applications and technologies for the energy sector—
    (i) to identify and mitigate vulnerabilities, including—
      (I) dependencies on other critical infrastructure; and
      (II) impacts from weather and fuel supply; and
    (ii) to advance the security of field devices and third-party control systems, including—
      (I) systems for generation, transmission, distribution, end use, and market functions;
      (II) specific electric grid elements including advanced metering, demand response, distributed generation, and electricity storage;
      (III) forensic analysis of infected systems; and
      (IV) secure communications;
  (B) to leverage electric grid architecture as a means to assess risks to the energy sector, including by implementing an all-hazards approach to communications infrastructure, control systems architecture, and power systems architecture;
  (C) to perform pilot demonstration projects with the energy sector to gain experience with new technologies; and
  (D) to develop workforce development curricula for energy sector-related cybersecurity."
- The "Energy Efficient Government Technology Act" (H.R. 1420) would require "each Federal agency…to develop an implementation strategy (that includes best practices and

measurement and verification techniques) for the maintenance, purchase, and use by the Federal agency of energy-efficient and energy-saving information technologies at or for federally owned and operated facilities, taking into consideration the performance goals established" by the Office of Management and Budget (OMB).s

FTC Oversight Hearing

Key Points:

- *The House subcommittee to sets the FTC's funding examines the agency's performance on privacy, data security, and antitrust issues*
- *FTC Chair said the $40 million funding increase in House funding package would be appreciated but would be devoted mostly to increasing costs the agency is facing*

The House Appropriations Committee's Financial Services and General Government Subcommittee held a hearing titled "Federal Trade Commission: Protecting Consumers and Fostering Competition in the 21st Century" with Federal Trade Commission (FTC) Chair Joe Simons and Commissioner Rohit Chopra.

Chair Mike Quigley (D-Il) remarked that the FTC has not appeared before the subcommittee in seven years but is one of the most important agencies it funds. He added it has only grown in importance in recent years with enormous jurisdiction policing most sectors of the economy for "bad behavior" including investigating robocalls, data breaches, consolidation in the healthcare market, consumer privacy and other technology issues. Quigley declared that both Democrats and Republicans are concerned about privacy issues and whether tech companies are respecting their customers privacy choices and if they are choking off competition by favoring their own products or by buying competitors. He noted the FTC has taken some promising actions recently, including "high profile settlements" with Facebook, YouTube, and Equifax and an antitrust investigation into Facebook and possibly other companies. He said the subcommittee understands the challenges facing the FTC in policing huge swaths of the economy, and this is why the House's FY 2020 Financial Services and General Government appropriations bill proposes a $40 million increase in FTC funding, an increase of more than 10%. Quigley expressed his interest in hearing from the FTC on how it would invest these resources widely to get the best results for consumers. He asserted the subcommittee also has a stake in determining whether the FTC is using its current resources efficiently. Quigley acknowledged that the $5 billion settlement with Facebook is by far the agency's largest on privacy "but it doesn't seem to match the magnitude of the privacy violations" and it does not even represent a full month of revenue for the company. He stated that it is not clear that the corporate changes the FTC secured will head off future privacy violations. Quigley said similar questions could be raised about the YouTube settlement or the Equifax settlement over one of the largest data breaches in U.S. history that included only $31 million for alternative compensation. He posed the question of how the FTC can function in an economy dramatically different than the one of ten years ago. Quigley asked if the FTC could win larger settlements to obtain better redress for consumers or to signal to the market that the U.S. will not tolerate anti-competitive or deceptive behavior.

Ranking Member Tom Graves (R-GA) noted the FTC's two primary missions: 1) to protect consumers from unfair, deceptive, and fraudulent practices, including identity theft, false advertising, unwanted telemarketing calls, scams against the elderly; and 2) ensuring that U.S. markets are open and free. He noted that while the FTC has not appeared before the subcommittee for seven years, since 2018 95% of the FTC's decisions have been unanimous. Graves noted how the growing

complexity of technology has made the FTC's work harder but stressed the critical importance of technology companies acting in an open and transparent manner, protect consumer privacy, and do not engage in anti-competitive business practices. He stated the FTC must be careful not to stifle innovation while conducting its important work, which is a difficult balance to achieve. Graves claimed that Over-regulation of industries can hurt both growth and the well-being of consumers.

FTC Chair Joe Simons stated that "[o]n the consumer protection side, we are aggressively pursuing law enforcement on privacy and data security matters, including record-breaking settlements with Facebook, Google and YouTube, and Equifax." He explained that "[w]e have mainly used a 100-year-old statute—Section 5 of the FTC Act—to bring our privacy and data security actions, but our authority under Section 5 is limited." Simons stated that "[t]hese limitations have a critical effect on our ability to protect consumers, which is why we urge Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers." Simons said that "[i]n addition to privacy and data security cases, we continue to bring a broad range of enforcement actions addressing, among other issues, fraud against older adults, servicemembers, and other diverse and underserved communities."

Simons said that "[o]n the competition side, enforcement actions in the pharmaceutical sector continue to be a priority for us…[and] [c]ases like our "pay for delay" matters protect generic competition, which helps keep drug prices down." He asserted that "[t]o address concerns about the power of "Big Tech," we created the Technology Task Force within our Bureau of Competition to concentrate our expertise and better monitor and investigate conduct by technology platforms."

Simons thanked the subcommittee "for the additional $40 million for the FTC that is in the House FY2020 Financial Services and General Government appropriations bill" and asserted that "we will make good use of additional funding." Simons said that "[a]lthough $40 million is a very substantial amount, more than half of it might be needed to cover mandatory compensation increases, step increases, and non-compensation costs related to our agency operations—such as our Consumer Sentinel Services contract, our litigation support service, and additional expert witness fees." He said that "[t]he remaining portion would likely be used for adding personnel (in the neighborhood of 90 [full-time employees]), although the manner in which we add personnel would have to factor in the probability of the funding continuing in the future." Simons said that '[w]e would focus new staff additions to priority areas such as supplementing our privacy and enforcement divisions; hiring more technologists; doubling the size of our Technology Task Force; and hiring more economists."

FTC Commissioner Rohit Chopra stated that "[a]s Congress tackles some of the biggest challenges facing our economy, society, and even our national security, the Federal Trade Commission should be a critical piece of the puzzle." He declared that "[t]he stakes could not be higher." Chopra posed a series of policy questions:

- For example, how will we combat pharmaceutical industry abuses contributing to out-of-control drug prices that can mean the difference between life and death for patients?
- What can we do to make sure that Americans can get a pay raise in a competitive job market, rather than being squeezed by employer consolidation and non-compete agreements?
- How will we reverse the worrisome decline in new business formation and make sure that American entrepreneurs are not blocked by incumbents protecting their turf?

- How will we safeguard sensitive data from abuse and misuse by those here at home seeking profit and by those abroad seeking to do us harm?
- How will we deal with the rising dominance of Big Tech when it comes to fake reviews, facial recognition, fair competition, and so much more?

Chopra stated that "Congress is currently considering an increase in funding for the FTC, and I share Chairman Simons' commitment to use every resource effectively to deliver value for the public."

Chopra said that "[t]he FTC hearings that convened over the last year were a reminder of the importance of self- critical analysis…[and] [w]e must always be searching for ways to be more effective." He asked "[f]or example, what more can we do to leverage the resources and authorities of our federal and state law enforcement partners to win full redress for victims and accountability for corporations and their executives that broke the law?" He also posed the questions "[h]ow can we codify existing policy guidance and case law into clear rules so we can seek stiff penalties to be returned to taxpayers?" Chopra asked "[w]hat more can we do to protect honest businesses who play by the rules?" He said that "[w]e are actively thinking about new ways to use the authorities and resources that Congress has entrusted to the agency that solve problems in our markets."

Hearing on Antitrust in Digital Technology Markets

Key Points:

- *One of the two subcommittees in the Congress looking at antitrust and big tech holds its second hearing in September*

The Senate Judiciary Committee's Antitrust, Competition Policy, and Consumer Rights Subcommittee held its second hearing on the month on antitrust issues generally but its first on antitrust and anti-competitive practices in the technology field. These hearings come amidst a similar set of hearings being held by the subcommittee on the House Judiciary Committee with antitrust and anti-competition jurisdiction and with the Federal Trade Commission (FTC) and Department of Justice (DOJ) having leaked word of investigations into Facebook, Amazon, Google, and Apple.

Chair Mike Lee (R-UT) said there is "a bit of feeding frenzy these days in the world of antitrust when it comes to big tech." He said while he was encouraged by the FTC and DOJ's scrutiny of the "tech giants" have violated antitrust laws, he is also concerned that these efforts may "overshoot." Lee said one area where it is crucial to get the balance right is in mergers between digital platforms and nascent and potential competitors. He claimed that everyone wants to be sure that competition is not harmed in tech markets so all can enjoy the benefits of innovation and consumer choice, two things that distinguish this sector of the U.S. economy. Lee noted that platforms markets are prone to tipping, which can lead to durable market power and to barriers to entry, and so acquisitions by dominant platforms that "gobble up" would be rivals to eliminate them should be prevented. He contended that discerning these sorts of acquisitions from those that are beneficial is not an easy task. Lee argued that if tech mergers are restricted too much and prevent pro-competitive acquisitions, then the U.S, runs the risk of potentially harming the startup ecosystem that fuels many of the consumer innovations American enjoy today. Lee said he wanted to hear from witnesses on how to balance those two, competing interests. He asserted that the hearing from the week before with the FTC and DOJ confirmed what he has long believed: it makes no sense to split civil antitrust enforcement between two federal agencies. He added that both agencies conceded that it would be wasteful for both to investigate the same firm for the same conduct. Lee noted that the DOJ's head of its antitrust enforcement efforts claimed that the FTC and DOJ could split up a

monopolization investigation on the same entity by looking at different conduct. He claimed that a monopolization investigation cannot be split up and run "piecemeal." Lee said that a single agency must examine the totality of all offenses in obtaining or maintaining market power, and therefore is a waste of taxpayer dollars for two agencies to conducting investigations of the same entity for the same offenses no matter how efficient, well-intentioned, and diligent those agencies may be.

Ranking Member Amy Klobuchar (D-MN) reiterated her position that the U.S. has a monopoly problem as evidenced by the "startup slump" in that the country has experienced a record low number of startups for the last few decades. She expressed her belief that a major cause for this is the monopolization of many markets. Klobuchar cited a Brookings Institute study showing the lowest number of startups since 1979 and another study showing a 26% decline in the formation of new businesses since 2006. She contended that Americans understand that competition is vital to markets and necessary for the flourishing of the next great American business. Klobuchar said that it makes sense that large digital platforms are the center of attention for antitrust policymakers since they are ubiquitous. She said that these policymakers have heard how these platforms are treating consumers, suppliers, and the handful of competitors that are still independent. Klobuchar said the *Wall Street Journal* recently published an article on the techniques Facebook has used on its rivals as detailed by Snapchat's parent. She remarked that threatening competition is just one of the signs of how big tech is dominating the market. Klobuchar said she was less concerned that Lee about how the antitrust pie is cut, for consumers will "end up with a pie in their face" unless action is taken soon. She stated that while the FTC and DOJ have looked into large mergers, the hearing would likely focus on when smaller firms are bought that usually have lower revenues and may be below the merger filing requirements. Klobuchar said that if digital giants are using strategic mergers to snuff out potential competitors, the harm may not be immediately obvious but no less harmful in the long run. She noted a recent white paper showing that the top five tech firms have made over 700 acquisitions since 1987. Klobuchar acknowledged the difficult of prevailing against mergers with a conservative Supreme Court and limited resources.

The FTC's Bureau of Competition Director Bruce Hoffman acknowledged "[t]he latest round of technology-driven disruption, instigated in significant part by digital platforms, has caused some to question whether our competition laws and enforcement approaches can continue to protect consumers from anticompetitive conduct and mergers in fast-paced markets characterized by technological change." He stated that "[t]he Commission is cognizant of these concerns and is committed to applying our expertise, economic learning, and the flexibility of the antitrust statutes to ensure that digital platform and other technology markets remain competitive." Hoffman contended that "the antitrust agencies have successfully applied the antitrust laws to technology companies that engage in anticompetitive conduct so as to maintain their dominant positions, and we are committed to continuing that tradition going forward." He said that "[t]o address the potential challenges posed by digital industries, the Bureau of Competition's newly formed Technology Task Force (TTF) is marshalling resources and expertise from across the Commission…[and] is actively conducting investigations." Hoffman explained that the TTF is "also deepening our understanding of technology markets and strengthening our ability to protect consumers from anticompetitive conduct and harmful mergers in the digital technology space." He stated written testimony "describes the basics of antitrust analysis that the Commission can employ to prevent competitive harm in technology markets, including when reviewing acquisitions of nascent and potential competitors by digital platforms."

Hoffman explained

> A salient feature of tech companies is their dynamism, but the Commission is cognizant of the fact that digital platforms may have unique characteristics. The Commission also understands that, while the sale to an incumbent represents a valuable exit strategy for startups that encourages investment and innovation, established firms may seek to acquire nascent or potential competitors poised to challenge their market position. And…merger analysis under the Clayton Act accounts for these incentives as well as any dynamic features of competition among firms already in the market and those seeking to enter the market. In addition to the Clayton Act, the Sherman Act bars a firm from gaining or maintaining a monopoly position through anticompetitive conduct, including acquisitions that exclude nascent and potential threats to its dominance….acquisitions by monopolists of nascent competitive threats may violate Section 2 of the Sherman Act when they are "reasonably capable of contributing significantly to the defendant's monopoly power," unless outweighed by procompetitive justifications.

American Antitrust Institute President Dr. Diana Moss suggested "a number of policy proposals to address weak merger enforcement in the digital technology sector:

> 1. Stronger merger presumptions are needed for acquisitions in the digital technology sector and should be a leading tool for invigorating effective merger enforcement. These include the presumptions for acquisitions of nascent and potential rivals, as described above. But given that many of digital technology acquisitions are vertical mergers, stronger vertical presumptions should also be considered. This includes rebuttable presumptions surrounding the effect of high market share in upstream or downstream markets on enhancing incentives to foreclose rivals. And the structural presumption in highly concentrative horizontal mergers involving digital technology markets should be rigorously applied.
> 2. Retrospective analysis of consummated mergers involving digital technology acquisitions is essential for determining which consummated deals should be challenged. Retrospective analysis of mergers is vital for determining if certain digital technology mergers resulted in higher prices, lower quality, less choice, or slower innovation. If concerns are identified, the agencies should use the full scope of their authority to bring challenges to consummated mergers under Section 7 of the Clayton Act and use fully effective remedies to restore competition lost by the acquisitions.
> 3. Improved agency transparency on digital technology merger actions would provide valuable information to the business community, consumers, and entrepreneurs. This includes more expansive press releases and/or closing statements for important acquisitions where the agencies investigated but took no enforcement action. Appropriately framed explanations as to why the agencies reached the decisions they did would provide important information without hampering the agencies' flexibility in future transactions.
> 4. A "blue ribbon" committee should be formed and tasked with evaluating the need for a new Digital Markets Act. The committee would evaluate the goals and parameters of potential legislation for a sectoral oversight authority. This includes an independent regulatory body with authority to implement and enforcement any new regulation surrounding digital market privacy, access, and interoperability. The committee would also frame out how such a regulator would work with antitrust enforcers to advise on technical matters that affect competition.

George Mason University Antonin Scalia Law School Associate Professor John M. Yun offered these recommendations:

- The agencies should and must continue to vigorously enforce the antitrust laws. As a society, we want technology companies, both large and small, to behave properly and innovate

within the bounds of conduct that is based on the merits rather than based on the ability to control the market, keep competitors out, and lower consumer welfare. In other words, we want to make sure that companies are succeeding based on merit rather than anticompetitive conduct. The agencies play a large role in this objective. To that end, I believe an increase in funding to the FTC and DOJ's respective antitrust divisions should be seriously considered. In particular, I believe the agencies would benefit from hiring more economists from all fields and expertise including machine learning, econometrics, labor, and finance. Increasingly, data is becoming a part of every case and the agencies will likely save more by having in-house expertise rather than contracting with outside consultants—although economic consultants do excellent work for both the government and the parties.

- Of course, agency growth should be done in a deliberate and thoughtful manner as expansion beyond a certain point will result in bureaucratic diseconomies of scale. Thus, I would be weary of proposals to add a "technology" group or other non-core antitrust specialists—as this will inevitably lead to significantly larger bureaucracies and associated inefficiencies without, perhaps, large offsetting benefits.
- Another potential route is for the FTC to exercise its 6(b) authority, which allows the agency to require an entity to file "annual or special...reports or answers in writing to specific questions" regarding the entity's "organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals."44 This would allow the agency to get somewhat "behind the scenes" and determine how the assets of acquired firms are being used and the level of investment, or lack of investment, involved. At the very least, a 6(b) study would give policymakers greater insight and data for which to inform policy decisions and could fuel further research into merger retrospectives.
- Finally, I would advocate for greater transparency to the public and policymakers for all major agency decisions—beyond when complaints are issued. Rather, I would like to see detailed statements regarding the particular agency's rationale(s) when cases both close and have a consent agreement. For example, when the FTC closed the Google Search bias investigation in 2013, it issued a closing statement that I believe can serve as a model for future investigations.

EU's Highest Court Rules For Google

Key Points:

- *In the instant case, a global platform like Google need not remove information on an EU citizen under the EU's Right To Be Forgotten*
- *However, there may be cases where the public interest might outweigh the Right To Be Forgotten*

The European Union's highest court has ruled in favor of Google in its dispute with France's data protection authority on whether the company must remove an individual's information all over the world under the provisions of the General Data Protection Regulation (GDPR) known as the "right to be forgotten" in Article 17. In 2017, France's Commission nationale de l'informatique et des libertés (CNIL) brought an action claiming that Google's failure to remove information from all its search engine sites violated provisions requiring such entities to "de-reference" upon request under the predecessor to the GDPR. Google was fined €100,000 and then appealed. The Court of Justice of the European Union (CJEU) ruled for Google in holding that the search engine company need only de-reference in EU member states while taking additional efforts to make it harder for EU citizens to use a version of Google, say the Australian version, to circumvent a request to be forgotten. However, this ruling may have larger implications in future cases where companies like Google seek to limit the application of the GDPR to only the EU.

Google operates its search engine in most countries but often with an extension on the address to distinguish it from other versions of Google. For example, the Google available in France has the Google.fr domain name extension. In bringing an action against Google, CNIL claimed that if the search engine merely removed information from French citizens from Google.fr then the right to be forgotten would not be respected, for a French national could search for and obtain the same information on another version of Google.

As the CJEU noted, "[b]y decision of 21 May 2015, the President of the CNIL served formal notice on Google that, when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted on the basis of that person's name, it must apply that removal to all its search engine's domain name extensions." Google's offer to de-reference these requests in the EU was rejected by CNIL. However, "Google refused to comply with that formal notice, confining itself to removing the links in question from only the results displayed following searches conducted from the domain names corresponding to the versions of its search engine in the Member States." The CJEU explained "[b]y an adjudication of 10 March 2016, the CNIL, after finding that Google had failed to comply with that formal notice within the prescribed period, imposed a penalty on that company of EUR 100 000, which was made public."

In its judgment, the CJEU considered the following issues:

- Must the "right to de-referencing", as established by the [Court] in its judgment of 13 May 2014, [Google Spain and Google (C 131/12, EU:C:2014:317),] on the basis of the provisions of [Article 12(b) and subparagraph (a) of the first paragraph of Article 14] of Directive [95/46], be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46]?
- In the event that Question 1 is answered in the negative, must the "right to de-referencing", as established by the [Court] in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States …?
- Moreover, in addition to the obligation mentioned in Question 2, must the "right to de-referencing" as established by the [Court] in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the "geo-blocking" technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46], regardless of the domain name used by the internet user conducting the search?'

In the 2014 case between Google and Spain, the CJEU ruled on a dispute arising from a Spanish national's request to make information relating to the recovery of social security debts through a

real estate auction. The CJEU ruled that an EU citizen would, in most cases, have the right to seek a de-referencing of information on the internet unless there is a "preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question." In this case of Google v. CNIL, the CJEU expanded its previous ruling.

The CJEU noted that "[i]n a globalised world, internet users' access — including those outside the Union — to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself." The CJEU also acknowledged that "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. The court added that "the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world." The CJEU found that "there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction from a supervisory or judicial authority of a Member State, to carry out such a de-referencing on all the versions of its search engine." Moreover, the CJEU added "a search engine operator cannot be required...to carry out a de-referencing on all the versions of its search engine."

However, the CJEU ruled that "where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request." And, yet, the CJEU added

> EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights...a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.

Consequently, there may be cases where the public interest outweighs the right to be forgotten such that a Google or similar entity could be ordered to delete this information from its sites worldwide. It remains to be seen which instances these might be. And, of course, the EU could act to amend its laws and/or the GDPR to make the right to be forgotten include the de-referencing of all such material worldwide if a request is made.

New Ballot Initiative To Strengthen CCPA

Key Points:

- *The Organization that got the CCPA on the 2018 ballot is trying to get a stronger bill on the 2020 ballot*

- *If enacted via ballot, it would be very heard to weaken or dilute the new statute*

The organization that successfully got the California Consumer Privacy Act (CCPA) placed on the 2018 ballot in California is now seeking to repeat this feat by trying to get the "The California Privacy Rights and Enforcement Act of 2020" (CPREA) on next year's ballot. Californians for Consumer Privacy (CCP) released an annotated version of bill that represents in many senses a rewrite of the CCPA to make it much more consumer friendly and the version submitted to the California Attorney General's office. CCP head and funder Alistair Mactaggart has said he will seek 1 million signatures to get this bill on the ballot; last year his organization collected 600,000 to get its version of the CCPA on the ballot, or roughly twice the number necessary. Of course, like last year, should CCP succeed in getting a bill on the ballot, it could then use this leverage to get further CCPA changes enacted that are short of those in the sweeping CPREA. It is just too soon to tell what the CCP's endgame is.

CCP's website explained the changes to the CCPA it wanted to highlight:

- Create new rights around the use and sale of sensitive personal information, such as health and financial information, racial or ethnic origin, and precise geolocation.
- Provide enhanced protection for violations of children's privacy by tripling CCPA's fines for breaking the law governing collection and sale of children's private information and would require opt-in consent to collect data from consumers under the age of 16.
- Require much-needed transparency around automated decision-making and profiling, so consumers can know when their information is used to make adverse decisions that impact lives in critical ways, including employment, housing, credit, and even politics.
- Establish a new authority to protect these rights, the California Privacy Protection Agency, which will simultaneously enforce the law and provide necessary guidance to industry and consumers, many of whom are struggling to protect themselves in an increasingly complex digital ecosystem, where hacking and identity theft remain a terrible problem.
- Protect our democratic processes by fixing election disclosure laws and requiring corporations to disclose whether, and how, they use personal information to influence elections.
- Most importantly, it would enshrine these rights by requiring that future amendments be in furtherance of the law, even though I am only setting the threshold to amend at a simple majority in the legislature. While amendments will be necessary given how technically complex and fast-moving this area is, this approach respects the role of the legislature while still providing substantial protections for Californians from attempts to weaken the law and their new human rights.

In the "Findings and Declarations" section of the draft bill, CCP claimed:

- Even before the CCPA had gone into effect, however, businesses began to try to weaken the law. In the 2019-20 legislative session alone, members of the Legislature proposed more than a dozen bills to amend the CCPA, and it appears that business will continue to push for modifications that weaken the law. Unless California voters take action, the hard-fought rights consumers have won could be undermined by big business.
- Rather than diluting consumer rights, California should strengthen them, including by imposing restrictions on businesses' use of personal information and how long they can keep it, by allowing consumers to opt-out of the use of their sensitive personal information for

advertising and marketing, and by requiring businesses to correct inaccurate information about consumers.

- An independent watchdog whose mission is to protect consumer privacy should ensure that businesses and consumers are well-informed about their rights and obligations and should vigorously enforce the law against businesses that violate consumers' privacy rights.

Among other changes to the CCPA, the CPREA would

- Create a new right for consumers to request and have incorrect information corrected by a business.
- Impose a new duty on businesses to disclose whether a consumer's personal information is being used by that business for "political purposes" and the "name of the candidate or candidates, committee or committees, and/or the title or titles of the ballot measure or measures for which the consumer's personal information was used for political purposes, and whether the consumer's personal information was used to support or oppose the candidate, committee, or measure."
- Require businesses to disclose upon request "Whether the business is profiling consumers and using their personal information for purposes of determining eligibility for financial or lending services, housing, insurance, education admission, employment, or health care services, together with meaningful information about the logic involved in using consumers' personal information for this purpose."
- Expand a business's responsibility to meet a consumer's request to know " the categories of persons to whom [a consumer's personal information] was disclosed for a business purpose" in addition to the existing requirement to identify the "categories of personal information that the business disclosed about the consumer for a business purpose."
- Bestow on consumers the right "at any time, to not to use the consumer's sensitive personal information or disclose it to a service provider or contractor, for advertising and marketing."
- Stipulate that a business may not sell "the sensitive personal information of a consumer unless the consumer has affirmatively authorized the business to sell the consumer's sensitive personal information"
- Narrow a business's latitude in "charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer." Currently, this may occur if the the "difference is reasonably related to the value provided to the consumer by the consumer's data." If enacted the standard would be tightened to "directly related to the value provided to the business by the consumer's data."
- Harmonize the CCPA with AB 1564, a bill passed by the legislature last month to allow web only businesses to provide an email address for requests for information from consumers instead of a toll-free number as non web only businesses must do
- Incorporate the provisions of AB 1355, another recently passed bill, to require reasonable authentication measures to verify that a consumer is actually making a request for information
- Expand a consumer's right to request and receive all data a business holds on them subject to exceptions as opposed to the current CCPA language generally limiting such request to 12 months
- Clarify that a service provider or contractor are not required to reply to verifiable consumer request, but are required to assist businesses in doing so

- Provide that once a business receives a consumer's opt-out request for advertising and marketing purposes, then the business may communicate this opt-out to any other entities authorized by the business to collect information from the consumer
- Raises the threshold for entities buying and selling personal information for purposes of being covered by the CCPA from 50,000 to 100,000 people or households
- Establishes a new category of protected information: "Sensitive personal information"
- Specifies that "[t]he implementation and maintenance of reasonable security procedures and practices following a breach does not constitute a cure" for purposes of stopping a consumer from suing
- Creates a new California Privacy Protection Agency and authorizes this body to levy "an administrative fine of not more than two thousand five hundred dollars ($2,500) for each violation, or seven thousand five hundred dollars ($7,500) for each intentional violation or violations involving the personal information of minor consumers....in an administrative enforcement action"
- Strike the requirement that the CA attorney general provide businesses with "guidance on how to comply with the provisions of this title
- Task the attorney general with crafting additional regulations to effectuate the new requirements of the CPREA

Changes to the California Code made by ballot initiative are much harder to change or modify than the legislative route for enacting statutes. Notably, the CPREA would limit future amendments to only those in furtherance of the act, which would rule out any attempts to weaken or dilute the new regime. Consequently, industry and allied stakeholders can be expected to fight this ballot initiative.

Committee Delves Into Online Disinformation

Key Points:

- *A committee began its examination of deepfakes and the possibility that they may accelerate the surge of disinformation on the internet*

The House Science, Space and Technology's Investigations and Oversight Subcommittee held a hearing titled "Online Imposters and Disinformation," a day after the full committee marked up a bill that "directs the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to support research to accelerate the development of technologies that could help improve the detection of [deepfakes]" according to the bill's sponsor.

Subcommittee Chair Mikie Sherrill (D-NJ) noted that "[r]esearchers generally define misinformation as information that is false but promulgated with sincerity by a person who believes it is true." She said that "[d]isinformation, on the other hand, is shared with the deliberate intent to deceive." Sherrill said that "the concepts of disinformation and online imposters are almost one and the same." She stated that "[w]e are seeing a surge in coordinated disinformation efforts particularly around politicians, hotbutton political issues, and democratic elections…[and] [t]he 2016 election cycle saw Russian troll farms interfering in the American discourse across Facebook, Twitter, Instagram, Youtube and beyond, trying to sway public opinion for their preferred candidate." Sherrill said that "at the same time, they were after something else much simpler: to create chaos." She stated that "[b]y driving a wedge into the social fissures in our society, sowing seeds of mistrust about our friends and neighbors, exploiting social discord, they think they might destabilize our democracy and allow the oligarchy to look a little more attractive by comparison." Sherrill stated that "[w]hen

I was a Russian policy officer in the Navy, I learned how central information warfare is in Russia's quest to dominate western nations…[a]nd unfortunately, modern technology makes information warfare a far easier proposition for our antagonists, foreign or domestic."

Subcommittee Ranking Member Ralph Norman (R-SC) said the hearing would "look at trends and emerging technology in this field, and consider research strategies that can help to detect and combat sophisticated deceptions and so-called 'deepfakes.'" He added that "[d]isinformation is not new…[and] has been used throughout history to influence and mislead people." Norman stated that "[w]hat is new, however, is how modern technology can create more and more realistic deceptions…[and] [n]ot only that, but modern disinformation can be spread more widely and targeted to intended audiences." He claimed thay "these fakes are growing more convincing and therefore more difficult to detect…[and] [a] major concern is this: as deepfake technology becomes more accessible, the ability to generate deepfakes may outpace our ability to detect them." Norman stated that "[a]dding to the problem of sophisticated fakes is how easily they can spread…[for] [g]lobal interconnectivity and social networking have democratized access to communication." He asserted that "[a]lgorithms used by social media platforms are designed to engage users with content that is most likely to interest them…[and] [b]ad actors can use this to better target disinformation." Norman said that "it is difficult to distinguish the techniques used in modern disinformation campaigns from the those used in ordinary online marketing and advertising campaigns." He contended that "[d]eepfakes alone are making online disinformation more problematic…[b]ut when combined with novel means for distributing disinformation to ever more targeted audiences, the threat is even greater." Norman said that "we are here today to discuss these new twists to an old problem and to consider how science and technology can combat these challenges."

State University of New York, University at Albany Professor Dr. Siwei Lyu explained that "[t]he term deepfake first emerged in late 2017 as the name of a Reddit account that began posting synthetic pornographic videos generated using an AI-based face-swapping algorithm." He noted that "[t]he term has subsequently become synonymous with three types of AI-generated impersonation videos: head puppetry, face swapping, and lip synching. Lyu stated that "[i]t is not an exaggeration to say that we are on the cusp of deepfakes being cheap, easy to produce, indistinguishable from real videos, and ready to cause real damages." He claimed that "[w]e therefore need a comprehensive and robust solution to this problem…[and] [t]he situation calls for continuous investment and perhaps an escalated funding level from the federal government to this strategically important research area." Lyu stated that "[t]he situation surrounding deepfakes may not turn out to be as severe as we are predicting now…[b]ut it is better safe than sorry."

University of California, Berkeley Professor Dr. Hany Farid proposed "several calls to action:

1. Funding agencies have to invest at least as much financial support to programs that seek to build systems to detect fake content as they do to programs in computer vision and computer graphics that are giving rise to the sophisticated synthesis technologies described above.
2. Researchers that are developing technologies that we now know can be weaponized should give more thought to how they can put proper safeguards in place so that their technologies are not misused.
3. No matter how quickly forensic technology advances, it will be useless without the collaboration of the giants of the technology sector. The major technology companies (including, Facebook, Google/YouTube, and Twitter) must more aggressively and proactively deploy technologies to combat disinformation campaigns, and more

aggressively and consistently enforce their policies. For example, Facebook's terms of service state that users may not use their products to share anything that is "unlawful, misleading, discriminatory or fraudulent". This is a sensible policy — Facebook should enforce their rules.

4. Lastly, we should not ignore the non-technological component to the issue of disinformation: us the users. We need to educate the public on how to consume trusted information, we need to educate the public on how to be better digital citizens, and we need to educate the public on how not to fall victim to scams, fraud, and disinformation.

Graphika Chief Innovation Officer Camille Francois stated that "[s]cience and technology have a crucial role to play in tackling this problem…[and] [t]he sheer volume of information on these platforms, and the speed with which it is shared, require new methods for campaign detection that can scale beyond our current capabilities." She stated that "[a]s our opponents become more effective at concealing their identities, we need to continuously innovate by creating forensic approaches that will be both accurate and difficult to undermine." Francois stated that "[a]nd for us to make real, measurable progress on these fronts, we need to address the thorny but essential problem of data availability." She said that "[t]he task at hand is to design a system that guarantees user security and privacy while ensuring that academic researchers, cybersecurity professionals, and human rights investigators can access the data they need to unlock our understanding of these threats and harness innovative ways to tackle the issue." She said that "[t]oday, we're very far from such a system."

U.S. and Allies Push For Cyber Norms

Key Points:

- *As two rival working groups began work on crafting international cyber norms, the nations behind one of them pushes its set of principles*

A few days after two United Nations (U.N.) groups began work on international cybersecurity norms, 27 nations led by the United States released a "Joint Statement on Advancing Responsible State Behavior in Cyberspace" the same day it co-hosted the second Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace with the Netherlands and Australia." These nations called on all nations to work towards creating a framework under which nation-states can be governed in cyberspace and come at a time when two U.N. created bodies are trying to determine a path forward for cybersecurity in international relations when cyber operations among some of the world's biggest nations seem to be accelerating.

In the Joint Statement, the nations asserted that "[s]tate and non-state actors are using cyberspace increasingly as a platform for irresponsible behavior from which to target critical infrastructure and our citizens, undermine democracies and international institutions and organizations, and undercut fair competition in our global economy by stealing ideas when they cannot create them." They stated that "UN member states have increasingly coalesced around an evolving framework of responsible state behavior in cyberspace (framework), which supports the international rules-based order, affirms the applicability of international law to state-on-state behavior, adherence to voluntary norms of responsible state behavior in peacetime, and the development and implementation of practical confidence building measures to help reduce the risk of conflict stemming from cyber incidents."

The 27 nations stated

> We underscore our commitment to uphold the international rules-based order and encourage its adherence, implementation, and further development, including at the ongoing UN negotiations of the Open Ended Working Group and Group of Governmental Experts. We support targeted cybersecurity capacity building to ensure that all responsible states can implement this framework and better protect their networks from significant disruptive, destructive, or otherwise destabilizing cyber activity. We reiterate that human rights apply and must be respected and protected by states online, as well as offline, including when addressing cybersecurity.

The nations stated that "[a]s responsible states that uphold the international rules-based order, we recognize our role in safeguarding the benefits of a free, open, and secure cyberspace for future generations." They warned that "[w]hen necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law…[and] [t]here must be consequences for bad behavior in cyberspace."

The nations called "on all states to support the evolving framework and to join with us to ensure greater accountability and stability in cyberspace."

The other signatories of the Joint Statement were Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Spain, Sweden, and the United Kingdom.

At the Second Ministerial Meeting, Deputy Secretary of State John Sullivan contended that

> The stakes are moving higher as more governments develop offensive cyber programs and as we see more frequent and severe cyber incidents. In 2017, we witnessed the reckless and uncontrolled WannaCry and NotPetya cyber attacks – both carried out by states – that caused billions of dollars of damage across Europe, Asia, and the Americas. It is clear states are increasingly deploying more sophisticated capabilities that threaten our cybersecurity.

Sullivan then argued that "[w]e as an international community must come together to mainstream and make universal well-established standards for state behavior in cyberspace and hold accountable those who transgress them."

The Joint Statement comes at a point when two U.N. bodies are looking to address cyberspace norms across national boundaries and tension between the two blocs of nations that supported the dueling efforts. Late in 2018, the U.N. passed two resolutions creating new bodies to develop an international agreement or set of agreements on what is considered acceptable and unacceptable cyber practices. Previous efforts largely stalled over disagreements between a bloc led by the U.S. and its allies and nations like China, Russia, and others with a different view on acceptable practices. Notably, unlike 2010, 2013 and 2015, the 2017 UN Group of Governmental Experts (GGE) could not reach agreement on additional voluntary, non-binding norms on how nations should operate in cyberspace.

A 2018 U.N. press release explained that two resolutions to create groups "aimed at shaping norm-setting guidelines for States to ensure responsible conduct in cyberspace:"

- the draft resolution "Developments in the field of information and telecommunications in the context of international security" (document A/C.1/73/L.27.Rev.1), tabled by the Russian Federation. By the text, the Assembly would decide to convene in 2019 an open-ended working group acting on a consensus basis to further develop the rules, norms and principles of responsible behaviour of States" offered by Russia.
- the draft resolution "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (document A/C.1/73/L.37), tabled by the United States…[that] would request the Secretary-General, with the assistance of a group of governmental experts to be established in 2019, to continue to study possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States" offered by the United States.

Thereafter, an Open Ended Working Group (OEWG) and the 2019 U.N. GGE were created.

Further Reading

- "Snap Detailed Facebook's Aggressive Tactics in 'Project Voldemort' Dossier" – *Wall Street Journal*. As part of its due diligence, the Federal Trade Commission (FTC) Is talking to Facebook's competitors like Snapchat about practices of the social media giant that may be anti-competitive and in violation of U.S. law. Snapchat has apparently been keeping files on Facebook's practices to undermine Snapchat in a file titled after the villain from the Harry Potter books and films. Facebook, of course, bought Instagram, a platform that most directly rivals Snapchat. However, the FTC may be focusing on an Israeli app, Onavo, Facebook bought in 2011 that promised users a virtual private network and reportedly allowed Facebook to examine user's personal information.
- "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies" – *The New York Times*. Apparently, the Federal Bureau of Investigation (FBI) has used National Security Letters (NSL) , an administrative subpoena to obtain information that does not need a judge's approval, on more companies than just those in Silicon Valley. NSLs usually comes with gag orders on the entity receiving them and entitle the FBI to all sorts of information. Documents obtained as part of a FOIA suit show the widespread use of NSLs in requests made to credit reporting agencies and banks.
- "Facebook CEO tries the quiet approach to soothing Washington" – *Politico*. Mark Zuckerberg put on a suit and tie to meet with key Members of Congress and President Donald Trump, but not Speaker Nancy Pelosi (D-CA), to discuss antitrust, data security, and privacy issues. However, the article is studded with on-the-record and off-the-record quotes suggesting Facebook's efforts are an attempt to hew to Washington's ways without actually yielding ground on any policy matters.
- "Attorney General Barr Seeks DOJ Facebook Antitrust Probe." – *Bloomberg*. Contrary to the agreement reached in May with the Federal Trade Commission (FTC) on which agency would investigate which tech giant, the Department of Justice is now looking into Facebook's conduct at the urging of Attorney General William Barr. Unnamed DOJ officials claim the DOJ is looking at different conduct than the FTC. DOJ may even look into Amazon, the other company that was supposedly the province of the FTC. In the May agreement, DOJ got Google and Apple.

- "Apple's Mac Pro Tariff Relief Requests Approved Despite Trump Opposition" – *Bloomberg*. Despite the President tweeting otherwise, the U.S. Trade Representative granted tariff relief to Apple for the importation of its Mac Pro.
- "How Huawei aims to convince U.S. companies it's not a Chinese spying tool" – *The Washington Post*. The Chinese tech giant is now waging a traditional lobbying/public relations campaign in the U.S. to counter the Trump Administration and Congress's sanctioning of the company. The success in the U.S. may be beside the ;point; the campaign may be to convince nations around the world that U.S. concerns about the security of their products are meritless.
- "How Google Changed the Secretive Market for the Most Dangerous Hacks in the World" – *Motherboard*. Google hired some of the world's best hackers for its Project Zero to find the vulnerabilities in its software and products and for competitors, too. It's just not clear if this is entirely a pro bono exercise for the tech world.
- "China Scores Businesses, and Low Grades Could Be a Trade-War Weapon" – *The New York Times*. China's Communist Party is introducing a system of social credit that can be used to deny businesses and individuals access to credit or other banking services if their data profile returns a low score. This system is already being used against U.S. firms in China.
- "Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers" – *Recode*. Amazon will try to persuade Capitol Hill to adopt its still to-be-written statute on facial recognition technology. Critics claim the company is trying to get weak federal standards enacted that would speed the adoption of facial recognition.
- "Revealed: how TikTok censors videos that do not please Beijing" – *The Guardian*. TikTok's parent, ByteDance, removes content from the platform as a matter of policy that might upset Beijing (e.g. posts mentioning Tiananmen Square).