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

Privacy Legislation Developments

For this week, let's revisit a House bill, the "Information Transparency & Personal Data Control Act" (H.R. 2013) that we examined in our September 5 edition. This bill is sponsored by Suzan DelBene (D-WA) and cosponsored by 22 other House Democrats. DelBene worked in Washington state's technology sector before transitioning to public service, including a stint with Microsoft. At present, this is not a bipartisan bill and consequently may be viewed as one of the House Democratic bills released this Congress.

This bill's profile was raised a bit last week the New Democrat Coalition, "the largest ideological House caucus…more than forty percent of the Democratic Caucus" according to their website, have formally endorsed H.R. 2013. The group says of itself: "[t]he New Democrat Coalition is made up of 104 forward-thinking Democrats who are committed to pro-economic growth, pro-innovation, and fiscally responsible policies." In their press release, the New Democrat Coalition summarized H.R. 2013 thusly:

> This bill will give people control over their most sensitive information and improve enforceability. This legislation requires the Federal Trade Commission (FTC) to mandate disclosure from companies on what information they are collecting and why, especially if it is being shared with another party. The primary sponsor of the "Information Transparency & Personal Data Control Act," Suzan DelBene, serves as the Vice Chair for Policy Coordination for the New Democrat Coalition.

And, while the New Democrat Coalition may be the largest single group among House Democrats, their endorsement does not necessarily mean H.R. 2013 will now become the party's de facto bill. Firstly, Speaker Nancy Pelosi (D-CA) has said she will oppose any bill that would weaken strong state laws like those in California under the soon to take effect "California Consumer Privacy Act" (CCPA) (A.B. 375). This is a position shared by a number of Democrats in the House or Senate. H.R. 2013 is not nearly as stringent a bill as the CCPA even though it does not entirely preempt state laws, so in order for this bill to pass the House, the bill itself would need to change or Members like Pelosi would need to soften their position. Also 23 of the New Democrats are from California and would likely feel pressure from some California stakeholders to oppose any bill that would weaken the CCPA and quite possibly pressure from the Speaker herself, too. Moreover, DelBene does not sit on House Energy and Commerce, the primary committee of jurisdiction, and it is more likely than any bill the House considers will be drafted by the Democrats on the committee such as Chair Frank Pallone Jr (D-NJ) and Consumer Protection and Commerce Subcommittee Chair Jan Schakowsky (D-IL).

As explained when we analyzed H.R. 2013:

> Generally, this bill would require that all data "controllers" must secure opt-in consent from consumers to collect, use, share, or sell their "sensitive personal information" subject to significant exceptions. But, beyond these exceptions, controllers could largely collect and

> share these types of data once consent has been provided by a consumer. Despite the seemingly robust opt-in and transparency requirements, there are some significant exceptions to the general rule that consumers must opt-in before controllers may collect and share their sensitive personal information, namely "opt-in consent shall not apply to the processing, storage, and collection of sensitive personal information or behavioral data in which such processing does not deviate from purposes consistent with a controller's relationship with users as understood by the reasonable user." Controllers would need to draft and publish their data usage, security, and privacy plans, and then be audited annually by independent, third-parties. The FTC would implement and oversee this new regime with state attorneys general being able to bring enforcement actions if the FTC does not act. Controllers who violate the new standards would be subject to enforcement including fines in the first instance and injunctive and equitable remedies under the FTC Act.

And there were also developments regarding another recently analyzed data privacy bill. Senator Ron Wyden (D-OR) formally introduced his bill, renamed as the "Mind Your Own Business Act," that is based substantially on the discussion draft released last fall, the "Consumer Data Protection Act." Wyden also released a one-page summary. As noted in our October 10 analysis of Wyden's discussion draft:

> This bill would vastly expand the power of the Federal Trade Commission (FTC) to police both the security and privacy practices off many U.S. and international multinational companies. The FTC would receive the authority to levy fines in the first instance, potentially as high as the European Union's General Data Protection Regulation of 4% of annual gross revenue. Moreover, the operative definition of the "personal information" that must be protected or subject to the privacy wishes of a consumer is very broad. The bill would also sweep into the FTC's jurisdiction artificial intelligence (AI) and algorithms (i.e. so-called big data). The "Consumer Data Protection Act" would also dramatically expand the types of harms the FTC could use its authority to punish to explicitly include privacy violations and noneconomic injuries.

In his press release, Wyden explained that "[t]he bill incorporates feedback Sen. Wyden received over the past year, and strengthens a number of pro-consumer provisions:

1. Strengthen the impact of the "Do Not Track" opt-out to stop companies from mining user data to target ads on behalf of other companies, which was allowed under the draft bill. A company could continue use data it holds for its own benefit (for example, examine user emails to develop a spell-checker, or improve its own service).
2. Extend "lifeline" protections for privacy-friendly services to low-income users. The bill ensures that privacy does not become a luxury good by requiring companies to offer privacy-protecting versions of their products for free to consumers who are eligible for the FCC's Lifeline program. Companies will be able to recoup this lost income by charging higher-income consumers a slightly higher fee for privacy-friendly services.
3. Permits state attorney generals to enforce the regulations created by the bill to get more cops on the privacy beat.
4. Creates a right of action for protection and advocacy organizations. Each state will be able to designate one "protection and advocacy" organization that can file civil suits against companies that violate privacy regulations. This provision would allow dedicated watchdogs to sue companies over privacy violations on behalf of consumers. The bill allows the FTC to distribute some of the money it collects in fines to the designated nonprofits.

5. Levies new tax penalties on companies whose CEOs lie about privacy protections. Companies whose executives are convicted will have to pay a tax based on the salary they paid to the officials who lied.
6. Clarifies that the bill does not preempt any state law."

As we also noted in terms of outlook for Wyden's discussion draft, which seems also to be the case for the "Mind Your Business Act:"

> This bill is likely the outer bounds desired by the most ardent privacy and civil liberties advocate, and therefore is highly unlikely to get enacted in its current form. Other Democratic bills are far more modest in scope, and few of them address both security and privacy. The chances of enactment are very low, but Congressional interest in privacy legislation will continue because of the GDPR and the California Consumer Privacy Act.

Section 230 Hearing

On October 16, the House Energy and Commerce Committee's Communications and Technology and Consumer Protection and Commerce Subcommittees held a joint hearing on Section 509 of the "Telecommunications Act of 1996" (P.L. 104-104) (aka the Communications Decency Act) that provides protection from legal liability for most online content moderators and fora. This provision has come under increasing scrutiny over the last few years as lawmakers and policymakers on the left and right have advocated for a possible rewrite of this liability shield in response to large social platform's seeming inability or unwillingness to take down offensive content in a timely fashion.

In the Democratic memorandum, staff explained

- Congress passed what became Section 230 of the Communications Decency Act (CDA 230) on February 8, 1996. CDA 230 enables websites to more freely moderate content online by generally providing immunity for online platforms for content posted by users. That means platforms are mostly not held liable for third-party content posted on their websites, with some relevant exceptions.
- The immunity works in two ways. First, CDA 230 prohibits courts from treating "an interactive computer service"—a web-based platform—"as the publisher or speaker" of material posted on the site by third-parties. Second, CDA 230 prohibits courts from holding websites liable for removing—in good faith—content that the websites found to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."
- CDA 230 does not protect a website from liability for its own content.CDA 230 does provide some exceptions to this immunity. Websites may still be held liable for third-party content that violates: (1) federal criminal law; (2) intellectual property law; (3) the Electronic Communications Privacy Act; and (4) certain laws prohibiting sex trafficking.

In the Republican memorandum, staff explained

> The Communications Decency Act (CDA) was enacted as Title V of the Telecommunications Act of 1996. Much of the original Title V was struck down, but a key section remains—Section 230. Section 230(c)(1) of the Communications Act provides a liability shield to "interactive computer services" from being treated as a publisher or speaker of any information provided by another information content provider, often interpreted to mean

> "user generated content." Section230(c)(2)of the Communications Act provides a civil liability safe harbor for "interactive computer services" that voluntarily, in good faith, take actions to restrict access to obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable content.

Communications and Technology Subcommittee Chair Mike Doyle (D-PA) said that online content moderation has largely enabled the internet experience consumers know today. He said that the platforms consumers visit have been enabled by user-generated content as well as the ability to moderate this content and create communities. Doyle remarked that Section 230 of the CDA has enabled that ecosystem to evolve by giving online companies the ability to moderate content without equating them to the publisher or speaker of that content. He added that this has led to the creation on massive online communities with millions and billions of people to come together and interact. Doyle asserted that the issues presented by Section 230 are complex, and some of the witnesses have argued that Congress should amend these provisions to address criminal activity, disinformation, and hate speech. He noted his agreement that these are serious issues. Doyle said his hometown of Pittsburgh has been affected by hate speech where a year ago a shooter motivated by extremist views shot Americans at a synagogue in what proved to be the deadliest attack on Jews in U.S. history. He stated that a similar shooting in New Zealand was streamed on social media sites. Doyle said that while many sites moved to quell the spread of that content, others did not move fast enough and the algorithms meant to promote sports highlights and celebrity selfies helped to amplify a heinous act. Doyle said that in 2016 foreign adversaries used the power of these platforms against the U.S. to disseminate disinformation to foment doubt in order to sow division and install distrust in our leaders and institutions. Doyle said it is clear that everyone needs to do better, and he encouraged social media platforms to "step up" to address the concerns of those noting the disturbing impact that the content on these platforms is having on society. He contended that Section 230 does not just protect the largest platforms or the fringe websites, but it also enables comment sections on individual blogs and leave free and honest reviews. He claimed this sort of discussion has enriched American lives and democracy. Doyle said that the ability of marginalized voices to be heard cannot be overstated. He added that these platforms have allowed people to speak truth to power.

Communications and Technology Subcommittee Ranking Member Bob Latta (R-OH) claimed that the hearing was a continuation of a discussion started last Congress as to how ensure that there is transparency and accountability for the hundreds of millions of Americans using the internet today. He stated that the witnesses represented an ideal balance of stakeholders. Latta said he wanted to be clear in saying that Congress should not repeal Section 230 nor is he advocating for niche carveouts that could lead to the slippery slope of the death by a thousand cuts that would ultimately upend the internet industry. He stated that before the committee discusses how to make nuanced, modest changes to the law, the committee needed to understand how things reached the current point. Latta noted that the original CDA also barred lewd and objectionable content, but these provisions were subsequently struck down by the Supreme Court. He asserted the original intention behind the CDA was to allow parents to co troll the content that entered their homes. Latta said it was unfortunate that courts interpreted Section 230 very broadly by absolving platforms of any responsibility for policing their content and have hidden behind procedural tools and abdicated their responsibilities. He stated that some platforms have done well, but other have not. Latta said the hearing would ideally focus on how Section 230 helps platforms in taking down content or if they have their own tools often in the form of terms of service. He claimed that Congress should look at means to ensure that platforms are held responsible for ensuring their content is not harmful but without harming the environment within which has allowed startups to flourish.

Consumer Protection and Commerce Subcommittee Chair Jan Schakowsky (D-IL) stated that the internet has improved the lives of Americans in many, many ways and enabled Americans to more actively participate in society, education, and commerce. She remarked that Section 230 has been at the heart of U.S.' internet policy for over 20 years. Schakowsky stated that many have claimed that these provisions have allowed free speech to flourish allowing the internet to grown into what it is today. She noted in the early days of the internet, this language was intended to help platforms moderate user generated content, especially illegal, offensive, or dangerous material. Schakowsky said the internet has come a long way since the enactment of Section 230. She stated that the amount and sophistication of user postings has increased exponentially. Schakowsky stated that unfortunately the number of who report experiencing extremism and online harassment, including sexual harassment, stalking, bullying, threats of violence, have gone up over the last two years 37%. She stated that extremism, hate speech, election interference, and other problematic content have likewise proliferated. Schakowsky said that the spread of this content is problematic and causes real harm that multi-billion-dollar companies like Facebook, Google, and Twitter cannot or will not fix. She said that another problem is that for-profit entities are now trying to use Section 230 as a li ability shield even though these cases have nothing to do with content moderation. Schakowsky noted a recent *Washington Post* article in which Uber executives seemed to be pondering on whether to use Section 230 to claim liability in a number of matters including labor, criminal, and local traffic matters. She said the Federal Trade Commission's (FTC) Section 5 powers on unfair and deceptive practices is also called into question as Section 230 may forestall agency action into the practices of some platforms. Schakowsky remarked of the inclusion of Section 230-type language being made part of trade agreements is inappropriate because Congress is examining issues related to the statute and besides this language is often incompatible with other nations' statutes. She claimed that Section 230 may no longer be achieving the goal of protecting consumers, and so it is her hope that "holistic solutions" can be discussed which does not include eliminating Section 230. Schakowsky called for a new look at Section 230 in light of the rise of big tech.

Consumer Protection and Commerce Subcommittee Ranking Member Cathy McMorris Rodgers (R-WA) stated in the early days of the internet two companies were sued for content posted on their sites by users. She said one company sought to moderate content but the other did not. McMorris Rodgers said the court held the company that did not police content was immune to suit while the other company was not immune. She said that it was thereafter that Congress decided to protect online content by granting liability protection to platforms which were also given the authority to moderate content that may be harmful, illicit or illegal. McMorris Rodgers said this liability shield has played a critical role in the development of the internet as small businesses and innovators have thrived online without the threat of frivolous lawsuits from bad actors looking to make quick buck. She claimed Section 230 is largely misunderstood. McMorris Rodgers asserted that Congress never intended to provide immunity to websites that are "neutral," and Congress never intended for platforms to be neutral conduits but, in fact, wanted platforms to moderate content. She said the liability protection was also intended to shield companies making good faith efforts to moderate material that is obscene, lewd, excessively violent or harassing. McMorris Rodgers asserted that Section 230 is supposed to institute a balance allowing all internet companies to innovate and flourish online while instituting incentives for companies to keep the internet clear of offensive and violent content by empowering these platforms to act in cleaning up their own sites. McMorris Rodgers said the internet also revolutionized free speech by allowing every American to have their voice heard and allowing them access to an almost infinite amount of information. She said she supports free speech and is sympathetic with some of the proposals to regulate content online, she

stated that she thinks they are ultimately not consistent with the First Amendment. McMorris Rodgers noted that Republicans fought successfully for a repeal of Fairness Doctrine, and she strongly cautioned those looking to implement such a policy for online content. She said she does not support gutting Section 230, but she said it is clear that it is incumbent on policymakers to have a discussion on striking the right balance on Section 230.

Boston University School of Law Professor Danielle Keats Citron explained that:

- In the early days of the commercial internet, lawmakers recognized that federal agencies could not possibly tackle all noxious activity online. Tech companies, in their view, were essential partners to that task. An early judicial decision, however, imperiled that possibility by ruling that platforms' content-moderation efforts increased the risk of liability. Lawmakers were appalled that online services would be penalized for self-regulation. Section 230 of the Communications Decency Act was a direct repudiation of that ruling. Congress wanted to incentivize private efforts to filter, block, or otherwise address troubling online activity. Section 230 provided that incentive by securing a shield from legal liability for under-or over-filtering "offensive" content.
- Section 230 has helped secure opportunities to work, speak, and engage online. But it has not been a clear win for civil rights and civil liberties. Its overbroad interpretation in the courts has undermined the statute's purpose and exacted significant costs to free speech and equal opportunity. Platforms not only have been shielded from liability when their moderation efforts have filtered or blocked too much or too little "offensive" or illegal activity, as lawmakers intended. But they also have been shielded from responsibility even then they solicit illegal activities, deliberately leave up unambiguously illegal content that causes harm, and sell dangerous products. The costs to free expression and equality have been considerable, especially for women, nonwhites, and LGBTQ individuals. Section 230 should be revised to condition the legal shield on reasonable content moderation practices in the face of clear illegality that causes demonstrable harm. That would return the statute to its original purpose—to allow companies to act more responsibly, not less.

Electronic Frontier Foundation Legal Director Corynne McSherry stated:

- Without Section 230—or with a weakened Section 230—online platforms would have to exercise extreme caution in their moderation decisions in order to limit their own liability. A platform with a large number of users can't remove all unlawful speech while keeping everything else intact. Therefore, undermining Section 230 effectively forces platforms to put their thumbs on the scale—that is, to remove far more speech than only what is actually unlawful, censoring innocent people and often important speech in the process.
- The effects of 2018's Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) offer an object lesson. FOSTA amended Section 230 to create new civil and criminal liability for platforms that host content about sex work at both the state and federal levels. It also broadly and ambiguously expanded federal criminal law to target online platforms where users discuss sex work and related topics.
- FOSTA's impact on Internet speech was apparent almost immediately after the law passed. Internet companies became significantly more restrictive toward speech discussing sex. The law threw harm reduction activities in the sex work community into a legal gray area, giving the organizations providing support to sex workers the unpleasant choice of taking on a great deal of legal risk or ceasing operations. Unfortunately, many of them chose the latter. Websites that sex workers relied on for sharing information about dangerous clients have gone offline, putting sex workers' lives at risk. At the same time, platforms presented with

new liability risks immediately moved to over-censor. For example, Craigslist completely removed its message boards dedicated to both personal ads and therapeutic services. The company could not individually review every post on those boards—and even if it could, it would not be able to reliably recognize every unlawful post—so it removed the boards altogether, punishing legitimate, lawful businesses in the process. Similarly, Tumblr—a community which many LGBTQ users have said was vital to them as youth—chose to ban all sexual content. Some smaller, niche personals sites either removed certain features or closed entirely.

- Our founders knew that it is impossible to craft laws that only target bad actors, which is why the First Amendment protects most speech, even distasteful or "indecent" speech. Private enforcers face the same problem, and it will only worsen if a failure to enforce perfectly could lead to legal liability.

Google's Global Head of Intellectual Property Policy Katherine Oyama asserted:

- As the Committee knows, §230 was first introduced in the 1990s as a result of a rising number of legal cases, including *Cubby, Inc. v. CompuServe Inc.*, and *Stratton Oakmont, Inc. v. Prodigy Services Co.*, which created a tenuous position for internet users and services. Courts found CompuServe not at fault for illegal user content because it had made no attempt to moderate, while holding Prodigy legally responsible after it had taken an "editorial" role in user content by moderating some of it. As a result of these cases and others, the law at that stage actually disincentivized taking action on truly harmful content online. §230 changed that calculus for platforms, incentivizing action against harmful content. The §230 "good Samaritan" provision was specifically introduced to incentivize self-monitoring and facilitate content moderation.
- In the intervening years, the importance of §230 to the US economy has only grown. It has generated a robust internet ecosystem where commerce, innovation, and free expression all thrive — while at the same time enabling providers to develop content detection mechanisms and take aggressive steps to fight online abuse. §230 is a key contributor to the US's $172 billion trade surplus in digital services. It is also critical in ensuring continued economic growth: A recent study found that over the next decade, §230 will contribute an additional 4.25 million jobs and $440 billion in growth to the economy. Furthermore, investors in the startup ecosystem -- who drive early investment in new technologies -- have said that weakening online safe harbors would have a recession-like impact on investment. §230 is also a differentiator for the US: China, Russia, and others take a very different approach to regulating and censoring speech online, sometimes including speech that is critical of political leaders.

House Judiciary Continues Anti-Competitive Investigation Into Big Tech

Last week, the House Judiciary Committee's Antitrust, Commercial, and Administrative Law Subcommittee held its third hearing into the market power of online platforms which focused on "The Role of Data and Privacy in Competition" as part of its "investigation into competition in digital markets."

Chair Jerrod Nadler (D-NY) stated that digital technologies have provided Americans with a remarkable array of services. He noted it has never been easier to post news and information, share content, and communicate with loved ones, all at a moment's notice. Nadler asserted that as with technological revolutions of the past, this transformation has upended the balance of power across the economy. He contended that it is important for Congress to study and understand how

these imbalances are affecting Americans, what are causing these asymmetries of power, and whether these new and growing inequalities are compatible with our democratic values. Nadler remarked that the committee's ongoing oversight of digital markets is a key part of this process. He said the hearing would examine how the use of data is contributing to the growing inequalities of power and how this affects competition. He said that as previous hearings have shown, a growing share of commerce and communications is controlled by a small number of companies. Nadler asserted that because these platforms are, in essence, large intermediaries, they are perfectly positioned to closely track each transaction and communication that passes through their channels. He stated that while intermediaries have long collected information on the economic activity that flows through their platforms, the large firms of the digital economy have unprecedented ability to track and surveil users across the internet. Nadler stated that this data collection includes information not only about a person's shopping and reading habits but also about the time they wake up and go to sleep, their precise location each hour of the day, and the content of their most private communications. He said that because several of these platforms derive the vast majority of their revenue from digital advertising, these firms also have an incentive to collect as much information as possible so that they can target consumers with precision. Nadler said that these troves of information can be used by companies in even more nefarious ways to discriminate on the user's race, gender, income, or otherwise to intrude on personal privacy. He explained that in light of these trends there are two questions he would like answered at the hearing:

- First, how are digital technologies and the constant data collection they enable affecting competition and is there something unique about digital markets that enables firms to acquire and maintain market power in novel ways. Nadler said that in digital markets maximizing data collection can provide a significant competitive advantage because a large and constantly growing set of user data allows firms to both improve existing products and services and to expand into new lines of business often with a competitive edge. Nadler said that frequently the companies with the most dominant are those that have captured the most data from as many sources as possible. He said scholars have described this as leading to winner take all markets with the first company to establish a competitive lead wins the market crushing any potential competition. Nadler asserted that competitors in digital markets have a strong incentive to collect as much information as possible as quickly as possible as part of a long-term strategy to compete in the marketplace and to achieve market dominance, which raises serious questions about whether it is desirable to have data be the key dimension along which companies are looking to compete.
- Second, how does data collection increase the ways that dominant companies can abuse their market power. Does the collection and use of data enable new forms of conduct that lawmakers and regulators recognize as anti-competitive. For example, platforms that serve as intermediaries for commerce have critical insight into their rivals' business models, a dynamic that raises significant competition concerns.

Antitrust, Commercial, and Administrative Law Subcommittee Ranking Member James Sensenbrenner (R-WI) said the hearing would focus on the roles that data play in privacy and competition and the ways the data of online consumers can be better protected. He said that data is in many ways the lifeblood of the internet, and numerous issues are swirling around the use of this data. Sensenbrenner said these include allegations that platforms that accumulate a large amount of data can function as barriers to entry for new platforms. He added that platforms holding large data bases can leverage that data to compete unfairly with third party competitors that are dependent upon their platforms. Sensenbrenner noted that incumbent platforms have pursued mergers with emerging competitors in order to kill off competition for data acquisition and market share. He stated his hope that the hearing could separate fact from fiction regarding these

allegations. Sensenbrenner reiterated his view that antitrust laws do not exist to punish success but rather to foster it. He cautioned antitrust regulators and Congress from extending antitrust laws in ways that punish success, suppressing innovation, and ultimately limiting consumer welfare. He added that these principles also apply to data privacy, and if Congress is going to legislate on this issue, it must get it right. Sensenbrenner said his views do not exist in a vacuum as many American and European governments have already acted, including the European Union with its General Data Protection Regulation (GDPR) and California with its California Consumer Privacy Act (CCPA). Sensenbrenner claimed that while well-intentioned, the GDPR is already producing substantial collateral damage to consumer well-being, innovation, and the health of the digital economy. He claimed it is likely the CCPA will have the same effect. He asserted that these results are avoidable, and the U.S. must put in place a better method of protecting consumer privacy online.

Antitrust, Commercial, and Administrative Law Subcommittee Chair David Cicilline (D-RI) noted that the committee launched a historic, bipartisan investigation into the state of the digital marketplace in June. He said the purpose of the investigation is to document anti-competitive behavior online, to determine whether the dominant firms are engaging in anti-competitive conduct, and to assess whether current anti-trust laws and enforcement levels are sufficient to address these problems. Cicilline stated that the committee has held a series of hearings, briefings, and Member roundtables to start this top-to-bottom review. He stated that the committee has requested documents and materials relevant to the investigation from the four dominant platforms. Cicilline explained that the committee received tens of thousands of pages of materials this week and will receive more in the weeks ahead. He added that hearings and roundtables would continue to ensure the goals of the investigation are met. Cicilline said this series of hearings are essential to the committee in executing its constitutional duties to ensure that anti-trust laws are working. He stressed that Congress and not the courts, agencies, or private companies, enacted the anti-trust laws, and Congress must be the body to determine whether current laws are keeping up with digital markets. Cicilline said the hearing was an opportunity for the committee to better understand a key component of digital markets: the role of data and privacy. He highlighted the international reports on competition in digital markets published on this issue that have noted that data is at the heart of the issue. Cicilline quoted the Australian Competition and Consumer Commission's "exhaustive" report which asserted that the "breadth and depth of user data collected by the incumbent digital platforms provides them with a strong competitive advantage creating barriers to rivals entering and expanding in relevant markets and allowing the incumbent digital platforms to expand into adjacent markets." He said the United Kingdom's Digital Competition Expert Panel similarly reported that large troves of data when combined with network effects may tip markets in favor of a single dominant platform, killing off competition. Cicilline referenced a University of Chicago report that cites the importance of access to data as a key factor in whether venture capital firms will invest in startups as those with less data receive less funding. He noted this has real consequences for firms that get locked out of the market and never get to offer new and innovative services. Cicilline also said there is broad agreement among anti-trust experts that data can be abused for anti-competitive purposes, and in some cases these tactics have created innovation "kill-zones" around dominant firms. Cicilline noted the hearing also provides the opportunity to examine the role of privacy in anti-trust and competition online. He asserted that while many services are billed as free, it is well known that consumers pay in the form of two valuable commodities: their personal data and their attention. Cicilline added that the prevalence of data usage and sharing techniques can indicate the lack of competition in markets. He contended that in a strong, competitive market, digital platforms would have strong incentives to deliver strong privacy standards, but in anti-competitive markets no such incentives exist. Cicilline claimed that competition and privacy are not mutually exclusive and that

they can and must be made to work in concert as the committee considers how to restore the internet to its full promise.

Federal Trade Commission (FTC) Commissioner Rohit Chopra stated "[a]s the Committee continues its investigation, it will be important for members of Congress to evaluate evidence with several things in mind, including:

> (1) Data has certain economic features that are unique and unlike other assets.
> (2) Most online services are not actually "free." While consumers and businesses are not paying with dollars, they are paying with data.
> (3) Competition is not a click away. Today's tech titans are wholly integrated throughout the digital world, such that people and businesses cannot avoid them.

Chopra noted that "[l]ast year, the FTC convened a series of hearings examining a range of competition and consumer protection issues in digital markets…[and] [t]he FTC staff has outlined next steps for these hearings, including policy outputs and deliverables." Chopra said that "I hope that the Commission will pursue work based on Section 6(b) of the Federal Trade Commission Act, which allows the agency to conduct industrywide investigations and studies and making its findings available to the public." He stated that "[g]iven its authority to prohibit unfair methods of competition and unfair or deceptive trade practices, the FTC is uniquely positioned to tackle the concerns associated with digital platforms." Chopra stated that "[t]he twin goals of competition and consumer protection are inextricably linked."

Harvard Kennedy School Professor of the Practice of Economic Policy Dr. Jason Furman stated that he "recently chaired the Digital Competition Expert Panel for the UK government that produced a report titled Unlocking Digital Competition" and is "currently advising the UK as they move forward with a key set of recommendations from this report, including the establishment of a Digital Markets Unit to act as a pro-competition regulator." Furman made "four points:

> (1) The major digital platforms are highly concentrated and, absent policy changes, this concentration will likely persist with detrimental consequences for consumers.
> (2) More robust competition policy can benefit consumers by helping to lower prices, improve quality, expand choices, and accelerate innovation. These improvements would likely include greater privacy protections given that these are valued by consumers. However, itis not clear that competition will be sufficient to adequately address privacy and several other digital issues.
> (3) More robust merger enforcement should be part of the solution to expanding competition, including better technical capacity on the part of regulators, more forward-looking merger enforcement that is focused on potential competition and innovation, and legal changes to clarify these processes for the courts.
> (4) A regulatory approach that is oriented towards increasing competition by establishing and enforcing a code of conduct, promoting systems with open standards and data mobility, and supporting data openness is essential. This is because more robust merger enforcement is too late to prevent the harms from previous mergers and antitrust enforcement can take too long in a fast moving market.

American Enterprise Institute Visiting Scholar Dr. Roslyn Layton stated that "Congress is right to focus on competition in the tech sector, but it won't achieve this with from third rate platforms mandate by government fiat." She claimed that "[i]nstead Congress should hasten the next technological revolution which will supplant the current incumbents." Layton stated that "[t]his can be done through policy that supports investments and incentives for next-generation technologies and removes the

market barriers to entrepreneurship, innovation, and enterprise." She asserted that "[h]ere the focus should be on fast-tracking 5G, the internet of things, artificial intelligence, blockchain, and security technologies." Layton stated that "[i]n summary rational privacy legislation could consist of

> (1) framework that protects Americans' Constitutional rights and freedoms for speech and commerce;
> (2) strengthened authority and budget for the FTC to develop risk-based privacy standards for the online economy (this would also include budget for more economists and technologists at the agency);
> (3) safe harbors that allow companies to migrate their operations to those standards,
> (4) investments and incentives for the development of privacy-enhancing technologies, and
> (5) consumer education and competency training.

Senate Commerce Majority Releases Reports Critical of CPSC's Data Security

Last week, Senate Commerce, Science, and Transportation Chair Roger Wicker (R-MS) released a Republican investigation into the data handling practices of the Consumer Product Safety Commission (CPSC) under a provision allowing the CPSC to collect and possibly release information regarding potential and possible product-related injuries. Senior CPSC made allegations that the agency was improperly handling these data, and a Committee investigation and report confirmed these allegations. However, in its letter to the agency, the Committee determined "accidental disclosures violating [the CPSC's enabling statute] occurred because of a lack of formal training, ineffective management, and poor information technology implementation at CPSC rather than deliberate malfeasance by CPSC employees."

The Consumer Product Safety Act (CPSA) (15 U.S.C. §§ 2051—2089) allows the CPSC to collect and obtain information related to the safety of a broad range of consumer products and to release this information as restricted by extensive requirements including consulting with the manufacturers of the products in question under 6(b) of the enabling statute. Consequently, the agency holds a trove of information some of which should not be made public. As the Committee explained

> The CPSC maintains several databases containing information regarding potential product-related injuries under the framework of the National Injury Information Clearinghouse. Members of the public are able to request information from the Clearinghouse, and such information can be provided subject to the requirements of section 6(b) of the CPSA. Section 6(b) prohibits the Commission from disclosing information from the Clearinghouse without taking reasonable steps to assure that the information is accurate, that disclosure of the information is fair in the circumstances, and that disclosure of the information is reasonably related to effectuating the purposes of the Act and of the other laws administered by the Commission. Section 6(b) requirements are meant to incentivize manufacturers to provide more safety information without fear of public backlash.

The agency explained in an April 2019 press release that "CPSC staff determined that information on approximately 11,000 unique manufacturers had been improperly disclosed since 2017…[and] immediately notified recipients and asked them to return or destroy of the information." Shortly before or contemporaneously with this public release, the CPSC alerted the Committee which maintains primary jurisdiction over the agency, and then the majority staff of the Committee launched an investigation. The Committee subsequently determined:

> Between December of 2017 and March 22nd, 2019, the CPSC clearinghouse made improper disclosures to 29 unique entities. The bulk of the disclosures went to two entities: Consumer Reports and a Researcher at Texas A&M University. These disclosures contained information on approximately 10,900 unique manufacturers, as well as street addresses, ages, and genders of approximately 30,000 consumers.

The Committee explained that "[a]fter reviewing hundreds of documents and emails and conducting multiple interviews, the Committee's investigation found that disclosures violating section 6(b) of the CPSA were due to a lack of training, ineffective management, and poor information technology implementation rather than deliberate efforts by CPSC employees." The Committee stated that "CPSC staff directly responsible for the disclosures had little to no knowledge of 6(b) requirements and received, processed, and completed information requests through the Clearinghouse independent of any managerial review." The Committee stated that "[t]hese employees are provided three different software applications to access and process relevant data without the necessary training on how to use these often confusing and idiosyncratic systems…[and] [w]e recommend that the CPSC implement the following procedures to ensure that Clearinghouse data requests are handled appropriately.

1. Conduct an internal review of training programs for new hires. New hires should undergo formal training on proper data-handling procedures as well as all applicable CPSA requirements.
2. Review and simplify information technology systems used to access and process data requests.
3. Implement clear and consistent review processes by which sensitive disclosures are reviewed by CPSC management, to potentially include CPSC Office of General Counsel (OGC) employees.

The CPSC has a spotty history regarding data security and information technology (IT). In the most recent Federal Information Security Modernization Act of 2014 Report to Congress, the Office of Management and Budget (OMB) detailed an independent assessment of the CPSC's information security program: "[t]he information security program of the Consumer Product Safety Commission was evaluated as not effective." OMB conceded that "CPSC improved its policies and procedures, implemented new cybersecurity solutions, and is actively working toward standardizing its risk documentation" but then listed all the ways in which the agency is failing to meet government-wide or agency-specific standards. OMB stated "CPSC has not:

- developed and maintained a comprehensive software and hardware inventory;
- documented and implemented baseline configurations for all agency hardware and software;
- applied patches in a timely manner;
- enforced multi-factor authentication;
- properly applied the Principle of Least Access;
- developed and maintained a business impact assessment and contingency and continuity plans;
- provided role-based security and privacy training to all applicable agency resources;
- implemented an organization-wide risk management program; or
- implemented processes to adequately protect PII throughout the data lifecycle.

OMB added that "IT contracts and agreements for goods and services lack required Federal Acquisition Regulation clauses and/or other provisions."

Likewise, the CPSC's Office of the Inspector General (OIG) has released critical evaluations of the agency's information security practices. A few weeks ago, the OIG listed among the four "most serious management and performance challenges facing the CPSC in FY 2020" "Enterprise Risk Management" and "Information Technology Security." Regarding the latter, the OIG explained:

> While the root causes of the data breach and unauthorized disclosure have not been fully identified, it is extremely likely that CPSC will need to consider a wide variety of process changes in addition to implementing new IT-based solutions to mitigate the risk of future incidents. OIG is aware that the agency has dedicated resources to address many of the issues identified in past FISMA and Penetration Testing reviews. These efforts demonstrate management's commitment to improving the agency's IT security.

It is likely given the timeline laid out that an early 2018 OIG-sponsored penetration test turned up the problematic 6(b) data handling practices. In this test, it was asserted "that the CPSC's security controls require improvement to more effectively detect and prevent certain cyberattacks." Incidentally, the firm that performed this penetration test started work in March and noted "early on in the testing phase [it] discovered improperly posted sensitive information which was publicly accessible via widely-used search engines and CPSC.gov…[and] notified the CPSC immediately about this discovery."

This investigation follows in the vein of the oft-expressed view of Republicans that nay data security or privacy legislation should pertain to government agencies, which are just as culpable as private sector entities when it comes to breaches and impermissible releases of information. Tellingly, Committee Democratic Members and staff are not associated with this investigation, suggesting a partisan focus.

Cantwell Seeks Answers and Precedents For FTC's Facebook Settlement.

In a letter, Senate Commerce, Science, and Transportation Committee Ranking Member Maria Cantwell (D-WA) pressed the Federal Trade Commission (FTC) pressed the FTC Chair Joseph Simons regarding her concerns about the $5 billion settlement reached with Facebook regarding its violations of consumer privacy arising from its partnership with Cambridge Analytica. Cantwell explained:

> I am concerned that the settlement lets Facebook off the hook for unspecified violations, and given the many public reports of Facebook's mishandling of consumer data, it is difficult to fully understand the impact of this provision of the settlement on the data privacy protection of the millions of U.S. consumers that have used and continue to use Facebook. Moreover, I am concerned that the release of Facebook and its officers from legal liability is far too broad and sets a dangerous precedent for future Commission actions.

Cantwell's concerns track those detailed in the two dissents from FTC Commissioners Rohit Chopra and Rebecca Kelly Slaughter.

Given Cantwell's position as the top Democrat on the committee through which privacy and data security legislation must pass to say nothing of the committee's oversight role of the FTC, she is positioned to influence and shape legislation. Her input could include language barring or dissuading the FTC from again granting blanket waivers of culpability for unknown actions and waivers of liability against corporate executives. Also, in pressing the agency to answer the below

detailed list of questions, she is keeping the spotlight on the FTC's actions in the data security and privacy space, possibly causing the agency to think twice before granting such a deal. It is also possible the FTC would seek to extract harsher terms in its next high profile settlement.

Cantwell stated that the Facebook settlement "has been criticized by a number of outside observers, and two of your fellow Commissioners, as insufficiently protective of consumers." She stated that "these parties have noted that this settlement may absolve Facebook from liability for past violations unknown at the time the FTC's 2019 Order was released…[and] may serve as an ineffective deterrent against future privacy violations."

Cantwell noted that "[m]ere weeks after the 2019 Order, we have learned that Facebook has been paying hundreds of outside contractors to transcribe clips of audio from users of its services potentially in violation of Facebook's data use policy going as far back as 2015." She asserted that "[t]his has raised substantial concern that fie 2019 Order will limit the FTC's ability to adequately address privacy violations by Facebook such as this one."

Cantwell added that "[i]t appears that the deal struck by the Commission and Facebook resolves all claims that Facebook previously violated the Commission's order imposed in 2012 ("2012 Order")— including all known and unknown claims not addressed in the 2019 Order or the Department of Justice complaint filed in this matter ("DOJ Complaint")." She explained that The resolution of such unknown claims under the2012 Order means that no matter what the Commission may learn about Facebook's previous practices- -such as human review of user-generated audio chats without clear disclosures to consumers and no matter how egregious a violation of the 2012 Order may have occurred—Facebook will not face another penalty by the Commission under the 2012 Order for such practices." Cantwell stated that "[i]t is my further understanding that, pursuant to the 2019 Order, the Commission has waived its ability to bring "known" claims against Facebook for unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act."

Cantwell stated that "the 2019 Order also specifically resolves all potential Section 5 claims against Facebook's officers and directors for violating the 2012 Order, including unknown claims, even though Facebook's officers and directors are not named as defendants in the DOJ Complaint." She said that "[t]he release of liability secured by Facebook and its officers and directors in the 2019 Order appears to be a departure from Commission standard practice when resolving consumer protection matters." Cantwell added that "[a]lthough the Commission's July 24, 2019 public statement on this matter suggests that other Commission settlements have included similar releases of liability, that statement does not cite a prior Commission settlement that released a defendant from unknown claims or that released individuals who are not named in the complaint."

I am concerned that the settlement lets Facebook off the hook for unspecified violations, and given the many public reports of Facebook' s mishandling of consumer data, it is difficult to fully understand the impact of this provision of the settlement on the data privacy protection of the millions of U.S. consumers that have used and continue to use Facebook. Moreover, I am concerned that the release of Facebook and its officers from legal liability is far too broad and sets a dangerous precedent for future Commission actions.

Cantwell asked Simons to "respond to the following questions:

Impact of Facebook's Release from Liability

1)How many complaints has the Commission received regarding Facebook's data privacy and security practices undertaken between the 2012 Order and 2019

Order? Is the Commission precluded from bringing an action against Facebook related to these practices for the period between the 2012 Order and 2019 Order?

2) Was the Commission staff aware of any allegations or complaints against Facebook for transcribing user audio potentially in violation of Facebook's user data policy? Is this conduct by Facebook considered a "known claim" under the 2019 Order?

Release of Liability Precedent

3) Please provide a list of other settlements of Commission consumer protection actions that resulted in releasing unknown claims for violations not alleged in the Commission complaint.

4) Please provide the number of Commission consumer protection actions that did not result in releasing unknown claims for violations not alleged in the Commission complaint.

5) Please provide a list of other settlements of Commission consumer protection actions that resulted in releasing individuals who are not named in the Commission complaint.

6) Please provide the number of consumer protection actions that did not result in releasing individuals who are not named in the Commission complaint.

Scope of the Commission's Facebook Investigation

7) Did the Commission staff interview, question, depose, or provide interrogatories to any Facebook officers or directors prior to executing this settlement? If so, please detail the names of those officers or directors and the scope of the investigation related to such individuals.

8) Did the Commission staff choose not to interview, question, depose, or provide Interrogatories to any Facebook officer or director who was involved in decision-making related to data practices subject to the 2012 Order? Please list such individuals and the reason for not including those individuals in the investigation.

Independent Oversight of Facebook

9) The 2019 Order mandates the creation of an "Independent Privacy Committee," comprised of "Independent Directors" from the Facebook Board.

a. What controls are in place to ensure that the "Independent Privacy Committee" will be truly independent from Facebook?

b. What steps will the Commission take to oversee the independence of the "Independent Privacy Committee" or demand removal of the Independent Privacy Committee' s members?

10) The 2019 Order mandates 'initial and biennial" assessments or the Facebook privacy program from "one or more qualified, objective, independent third-party professionals," referred to as the "Assessor.' The 2019 Order also gives Facebook the authority through a majority vote of the Independent Privacy Committee, to remove the Assessor. The 2019 Order, however, does not appear to grant that same authority to the Commission.

a. Please explain why the 2019 Order does not contain a parallel removal provision for the Associate Director of BCP's Division of Enforcement or the Commission.

b. Does the Commission have policies or procedures for gauging the objectivity independence, or effectiveness of the Assessor? If so, please provide such policies or procedures.

LPTA Proposed Rule

Following on the heels of the final rule promulgated to restrict the use of Lowest Price Technically Acceptable (LPTA) contracts for many Department of Defense (DOD) contracts, the DOD, General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) have released a proposed rule that mirrors the DOD's final rule. This proposed rule would implement language from FY 2019 National Defense Authorization Act (NDAA) extending the restriction of LPTA to the rest of the federal government as previous NDAAs had tasked the Pentagon with drafting regulations. Consequently, this proposed rule does not pertain to the DOD but rather the rest of the federal government. Nonetheless, the proposed rule would direct agencies to avoid using LPTA in buying "Information technology services...[and] cybersecurity services" to the maximum extent possible" and there would be similar restrictions in the form of additional steps and analysis contracting officers must perform in order to use LPTA to buy cybersecurity and IT products. Comments are due on December 2, 2019.

The agencies explained that "Section 880 of the [FY 2019 NDAA] (P. L. 115-232, 41 U.S.C. 3701 Note) makes it the policy of the Government to avoid using LPTA source selection criteria in circumstances that would deny the Government the benefits of cost and technical tradeoffs in the source selection process." The agencies explained that "[e]xcept for DOD…the LPTA source selection process shall only be used when—

> (1) The agency can comprehensively and clearly describe the minimum requirements in terms of performance objectives, measures, and standards that will be used to determine the acceptability of offers;
> (2) The agency would realize no, or minimal, value from a proposal that exceeds the minimum technical or performance requirements;
> (3) The agency believes the technical proposals will require no, or minimal, subjective judgment by the source selection authority as to the desirability of one offeror's proposal versus a competing proposal;
> (4) The agency has a high degree of confidence that reviewing the technical proposals of all offerors would not result in the identification of characteristics that could provide value or benefit to the agency;
> (5) The agency determined that the lowest price reflects the total cost, including operation and support, of the product(s) or service(s) being acquired; and
> (6) The contracting officer documents the contract file describing the circumstances that justify the use of the lowest price technically acceptable source selection process.

In contrast, the DOD has additional requirement in using LPTA under the final regulations, namely

- Goods to be procured are predominantly expendable in nature, are nontechnical, or have a short life expectancy or short shelf life (See PGI 215.101-2-70(a)(1)(vi) for assistance with evaluating whether a requirement satisfies this limitation);
- The contract file contains a determination that the lowest price reflects full life-cycle costs (as defined at FAR 7.101) of the product(s) or service(s) being acquired (see PGI 215.101-2-70(a)(1)(vii) for information on obtaining this determination);

And, just like the DOD's final rule on LPTA, other agencies' "contracting officers shall avoid, to the maximum extent practicable, using the lowest price technically acceptable source selection process in the case of a procurement that is predominantly for the acquisition of—

> (1) Information technology services, cybersecurity services, systems engineering and technical assistance services, advanced electronic testing, audit or audit readiness services,

health care services and records, telecommunications devices and services, or other knowledge-based professional services;
(2) Personal protective equipment; or
(3) Knowledge-based training or logistics services in contingency operations or other operations outside the United States, including in Afghanistan or Iraq."

In order to provide context to how widely the DOD used LPTA contracts before these provisions were enacted, in November 2018, the Government Accountability Office estimated "that about 26 percent of DOD's contracts and orders valued at $5 million or more in fiscal year 2017 were competitively awarded using the LPTA process."

Further Reading

- "How to report on a data breach" – *Columbia Journalism Review*. A veteran tech journalist who has written about a number of the recent, major data breaches (Target, MySpace, Equifax, LinkedIn, eBay, JP Morgan Chase, Yahoo, and Sony) offers tips to other journalists that can serve those interested in the policy side of these issues, including how to best confirm that a hack has occurred and its extent and how to ethically confirm an email address or log-in information is part of a breach.
- "How to Stop the Abuse of Location Data" – *The New York Times*. Foursquare CEO Jeff Glueck lays out the principles Congress should enshrine in legislation regulating how the location data on smart phones and other devices is used, including a fiduciary duty that would bar the use of some location data (e.g. visits to Planned Parenthood):
    - First, apps on mobile devices should not be allowed to ask for location data unless they offer the user a clear service that depends on that data.
    - Second, a new privacy law must require greater transparency around what consumers are signing up for and how their data will be used.
    - Third, a privacy law must establish the obligation and duty on those collecting location data (even with consent) to "do no harm."
    - Moreover, all location companies should be required to protect consumer data with appropriate security steps, and blur or minimize data sharing in ways to enhance privacy.
- "My Family Story of Love, the Mob, and Government Surveillance" – *The Atlantic*. Former Assistant Attorney General and Harvard Law School Professor Jack Goldsmith makes amends with his stepfather, Chuckie O'Brien, an intimate of Teamsters head Jimmy Hoffa, by tracing the history of the U.S. government disregarding constitutional and statutory constraints on surveillance in the name of fighting national security and criminal threats. Once surveillance abuses come to light, Congress institutes new limits while legalizing some of the previously illegal practices. In the name of national security, a future administration violates these limits, and the cycle begins anew. Goldsmith's reluctant conclusion is "The executive branch does what it thinks it must, including conduct robust surveillance, to meet our demands for safety. The technology of surveillance races ahead of the law of surveillance, which tries to catch up in spurts, and often does an admirable job of curtailing old abuses. But the law cannot eliminate ever-growing threats, and security is elemental."
- "California blocks police from using facial recognition in body cameras" – *San Francisco Chronicle*. California Governor Gavin Newsom signed A.B. 1215 which will bar police departments from using body cameras that utilize facial recognition or biometric information for three years. The bill's primary sponsor was motivated to act once Amazon's facial recognition technology, Rekognition, incorrectly identified 26 members of the California

legislature as criminal suspects. California is the third state after Oregon and New Hampshire to ban this technology for police departments, and Oakland and San Francisco already bar this practice.

- "Is Amazon Unstoppable?" – *The New Yorker*. The magazine takes a very long, very deep look at the online retailer, its culture, its impact, its labor practices, and its CEO. The upshot is that Amazon is poised to fight tooth and nail against tighter regulation at the federal and state level despite historic tides that may be running against them if previous patterns of American capitalism repeat.
- "Jeff Bezos's Master Plan" – *The Atlantic*. A deeper look at Jeff Bezos and Amazon.
- "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials" – *Reuters*. U.S. officials leaked word of at least the third cyber attack on Iran in response to provocation. In this case the September attack on a Saudi oil facility prompted an attack on Iran's propaganda apparatus.
- "Accused Capital One hacker had as much as 30 terabytes of stolen data, feds say" – *cyberscoop*. The hacker who stole the identity information of millions may have also penetrated other entities, often by probing firewalls for weaknesses that would give her access to the cloud.