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

Spotlight: A Privacy Bill A Week

Last week, we dived into 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. This week, we will analyze the most stringent, most pro-consumer bill on privacy that I have seen introduced in this or the last Congress.

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

The "Consumer Data Protection Act" would dramatically expand the types of harms the FTC could use its authority to punish to explicitly include privacy violations and noneconomic injuries. Currently, the FTC must use its Section 5 powers to punish unfair and deceptive practices, or another statutory basis such as COPPA, to target the privacy practices it considers unacceptable. Wyden's bill would allow the FTC to enforce the FTC Act, as amended by his bill, to punish "noneconomic impacts and those creating a significant risk of unjustified exposure of personal information" as among those "substantial injur[ies]" made illegal. It is worth seeing the proposed language in the context of the section of the FTC's organic statute (i.e. 15 U.S.C. 45(n)):

> *(n) Standard of proof; public policy considerations*
>
> The Commission shall have no authority…to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury ***including those involving noneconomic impacts and those creating a significant risk of unjustified exposure of personal information*** to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition (emphasis added to differentiate the language the bill would add.)

The FTC's new authority would likely be defined in court actions to test the outer limits of what constitutes "noneconomic impacts" and the types of substantial injuries that create a significant risk of unjustified exposure of personal information. If this language were enacted, undoubtedly industry groups and conservative advocacy organizations would zealously search for test cases to

try to circumscribe this authority as narrowly as possible. Finally, it bears note that this sort of language harkens back to the FTC's construction of its statutory powers in the 1960's and 1970's that was considered so expansive that a Democratic Congress reined in the agency and limited its purview.

The FTC's authority to levy civil fines through an administrative proceeding would be dramatically expanded along the lines of the EU's power to levy massive fines under the General Data Protection Regulation. Notably, without securing a court order, the agency could impose civil fines as part of a cease and desist order which shall be the higher of $50,000 per violation or 4% of the annual gross revenue of the offender in the previous fiscal year. The upper limits of such a fine structure get very high, very quickly. For example, a violation with 100,000 people affected yields an upper boundary of $5 billion assuming one violation per person. The privacy violations associated with Facebook's conduct with Cambridge Analytica affected 87 million worldwide, and again assuming one violation per person, the upper boundary of the fine the FTC could levy would be $4,350,000,000,000. However, the FTC would likely not exercise this power to the utmost possible fine but rather dial back the fine to a more reasonable but still punitive amount. Nonetheless, the FTC would have the ability to recover up to $50,000 per violation or 4% of gross annual revenue for any violations of cease and desist orders by filing an action in federal court.

Despite expanding the FTC's powers dramatically, those entities subject to the agency's new enforcement powers would not include many medium and small businesses. Covered entities are described as those entities with more "than $50,000,000 in average annual gross receipts for the 3-taxable-year period preceding the fiscal year" and the "personal information" of more than 1,000,000 consumers, and 1,000,000 consumer devices. Additionally, a covered entity may be an affiliate or subsidiary of an entity that meets the aforementioned qualifications. Finally, the term "covered entity" covers all data brokers or commercial entities "that, as a substantial part of their business, collects, assembles, or maintains personal information concerning an individual who is not a customer or an employee of that entity in order to sell or trade the information or provide third-party access to the information."

Additionally, a subset of these covered entities with more than $1 billion in annual revenues that "stores, shares, or uses personal information on more than 1,000,000 consumers or consumer devices" or those "that stores, shares, or uses personal information on more than 50,000,000 consumers or consumer devices" must submit annual data protection reports to the FTC. Those entities must report "in detail whether, during the reporting period, the covered entity complied with the regulations" the FTC will promulgate to effectuate the "Consumer Data Protection Act" and the extent to which they did not comply by detailing which regulations were violated and the number of consumers affected.

Each report must "be accompanied by a written statement by the chief executive officer, chief privacy officer (or equivalent thereof), and chief information security officer (or equivalent thereof) of the company" that certifies the report fully complies with the requirements of the new statute. If any such person certifies an annual data protection report while knowing it does not meet the requirements of this section or with intentional knowledge it does faces jail time and/or a personal fine based on income depending on which state of knowledge the actor had in falsely certifying a report. Any CEO, chief privacy officer, or chief information security officer that knowingly certifies a false report faces a fine of the greater of $1 million or 5% of the highest annual compensation for the previous three years and up to ten years in prison. Intentional violations expose these

corporate officials to the greater of a $5 million fine or 25% of the highest annual compensation for the previous three years and 20 years in prison.

Of course, falsely certifying knowing that a report fails to meet all the requirement exposes a person to less criminal liability than intentionally certifying. However, the substantive difference between knowing certification and intentional certification is not immediately clear. Perhaps the bill intends knowing to be constructive knowledge (i.e. known or should have known) while intentionality in this context means actual knowledge.

With respect to the information covered entities would need to safeguard, the bill defines "personal information," which is "any information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device," which is a very broad definition. Wyden's bill also defines "use," "share," and "store" in the context of personal information:

- "share"—
    - means the actions of a person, partnership, or corporation transferring information to another person, partnership, or corporation; and
    - includes actions to knowingly—
    - share, exchange, transfer, sell, lease, rent, provide, disclose, or otherwise permit access to information; or
    - enable or facilitate the collection of personal information by a third party.
- "store"—
    - means the actions of a person, partnership, or corporation to retain information; and
    - includes actions to store, collect, assemble, possess, control, or maintain information.
- "use" means the actions of a person, partnership, or corporation in using information, including actions to use, process, or access information.

The FTC would be required to promulgate detailed regulations discussed in more detail below within two years of enactment. This timeline may be more realistic than many of the other bills which task the agency with detailed, extensive rulemakings within a year, a deadline the FTC may have trouble meeting. Nonetheless, the agency could take the first year or even 15 months to draft proposed regulations for comment.

The bill would task the FTC with establishing and running a "Do Not Track" data sharing opt-out website that would stop covered entities from sharing a consumer's personal information subject to certain exceptions including the use of personal information acquired before a consumer opts out. These would be in the case when a covered entity needs to share the information to achieve the primary purpose under which the information was initially acquired. Additionally, this bar would be in effect for personal information a covered entity acquires from non-covered entities.

The FTC would also need to determine technological means that a consumer's opt-out on its website can be effectuated through web browsers or operating systems. The agency would also need to devise a method by which covered entities could determine which consumers have opted out, possibly through the development of an FTC Application Programming Interface (API). Thereafter, covered entities would have a duty to check at regular intervals the FTC's opt-out database to ensure they are honoring the consumers' decisions to opt out. Covered entities would not need to respect a consumer's desire to opt-out in the event of required legal disclosures they need to make to the government such as under warrants or subpoenas. The FTC would also need to "establish

standards and procedures, including through an API, for a covered entity to request and obtain consent from a consumer who has opted-out…for the covered entity to not be bound by the opt-out," including providing a list of third parties with whom personal information might be shared and a description of such information. And, if the covered entity requires consumers to consent to usage of their personal information before its products or services can be used, then the covered entity must "notify the consumer that he or she can obtain a substantially similar product or service in exchange for monetary payment or other compensation rather than by permitting the covered entity to share the consumer's personal information."

The FTC must also "establish standards and procedures requiring that when a non-covered entity that is not the consumer shares personal information about that consumer with a covered-entity, the covered entity shall make reasonable efforts to verify the opt-out status of the consumer whose personal information has been shared with the covered entity." Thereafter covered entities may only use or store this personal information if a consumer has not opted out on the FTC's website or if the covered entity has received the consumer's consent for non-covered entities to collect and share their information.

Additionally, the FTC must draft regulations detailing the "standards and procedures" covered entities and non-covered entities must follow "to request and obtain consent from a consumer…that clearly identifies the covered entity that will be storing or using the personal information and provides the consumer" at the time consent is ought. Consumers must be informed "in a form that is understandable to a reasonable consumer" detailing the entity from whom personal information is to be obtained, the type of personal information to be collected, and the purposes for which such information shall be used.

Certain acts would be prohibited. Covered entities could require consumers to change their opt-out election on the FTC's website in order to access products and services "unless the consumer is also given an option to pay a fee to use a substantially similar service that is not conditioned upon a requirement that the consumer give the covered entity consent to not be bound by the consumer's opt-out status." Moreover, this fee "shall not be greater than the amount of monetary gain the covered entity would have earned had the average consumer not opted-out."

Wyden's bill also marries data security requirements with privacy protections for consumers, a position articulated by a number of prominent Democrats. Notably, the FTC would need to promulgate regulations that

- require each covered entity to establish and implement reasonable cyber security and privacy policies, practices, and procedures to protect personal information used, stored, or shared by the covered entity from improper access, disclosure, exposure, or use;
- require each covered entity to implement reasonable physical, technical, and organizational measures to ensure that technologies or products used, produced, sold, offered, or leased by the covered entity that the covered entity knows or has reason to believe store, process, or otherwise interact with personal information are built and function consistently with reasonable data protection practices;

The FTC would also need to draft regulations requiring "each covered entity to provide, at no cost, not later than 30 business days after receiving a written request from a verified consumer about whom the covered entity stores personal information" a way to review any personal information stored, including how and when such information was acquired and a process for challenging the accuracy of any stored information. Additionally, these regulations would "require each covered

entity to correct the stored personal information of the verified consumer if, after investigating a challenge by a verified consumer…the covered entity determines that the personal information is inaccurate." Covered entities would also need to furnish a list of the entities with whom the consumer's personal information was shared and other detailed information, including the personal information of the consumer the covered entity acquired not from the consumer but a third party.

The "Consumer Data Protection Act" would also institute regulations and requirements related to the increasing use of so-called "big data," algorithms, machine learning, and artificial learning. The FTC would need to promulgate regulations mandating that each covered entity must "conduct automated decision system impact assessments of existing high-risk automated decision systems, as frequently as the Commission determines is necessary; and…new high-risk automated decision systems, prior to implementation." However, it would be helpful to examine the bill's definitions of ''automated decision system,'' ''automated decision system impact assessment,'' ''high-risk automated decision system'' and "high-risk information system." An "automated decision system":

- ''automated decision system'' means "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers.
- "automated decision system impact assessment" means a study evaluating an automated decision system and the automated decision system's development process, including the design and training data of the automated decision system, for impacts on accuracy, fairness, bias, discrimination, privacy, and security
- ''high-risk automated decision system'' means an automated decision system that—
    - taking into account the novelty of the technology used and the nature, scope, context, and purpose of the automated decision system, poses a significant risk—
        - to the privacy or security of personal information of consumers; or
        - of resulting in or contributing to inaccurate, unfair, biased, or discriminatory decisions impacting consumers;
        - makes decisions, or facilitates human decision making, based on systematic and extensive evaluations of consumers, including attempts to analyze or predict sensitive aspects of their lives, such as their work performance, economic situation, health, personal preferences, interests, behavior, location, or movements, that—
            - alter legal rights of consumers; or
            - otherwise significantly impact consumers;
            - involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;
            - systematically monitors a large, publicly accessible physical place; or
    - meets any other criteria established by the Commission in regulations…
- 'high-risk information system" means an information system that—
    - taking into account the novelty of the technology used and the nature, scope, context, and purpose of the information system, poses a significant risk to the privacy or security of personal information of consumers;
    - involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership,

genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;
- systematically monitors a large, publicly accessible physical place; or
- meets any other criteria established by the Commission in regulations…

Consequently, algorithmic decision-making would be swept into the FTC's new regime to govern privacy and data security. However, politically, this is not close to being on most Members' consciousness as being related to privacy and data security. This reality marks the "Consumer Data Protection Act" as among the most forward looking of the bills that have been introduced over the last year. And, yet it is likely that any privacy or data security bill Congress passes will not include such provisions; however, a state like California could decide to wade into this area, which, again like with privacy, this could force policymakers in Washington to consider an issue percolating up to the federal level from one of the state laboratories of democracy.

In terms of enforcement, the bill explicitly bars the use of any contracts contrary to the rights and requirements in the "Consumer Data Protection Act." Like virtually all the other bills on privacy, the FTC would be able to ask a federal court for civil fines for a first offense as high as a bit more than $40,000 per violation in addition to all the FTC's other powers.

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.

US/UK CLOUD Act Agreement Announced; US, UK, and Australia Press Facebook On Encryption

The U.S. Department of Justice (DOJ) and the United Kingdom's Home Ministry announced that the U.S. and U.K. have signed an agreement "that will allow American and British law enforcement agencies, with appropriate authorization, to demand electronic data regarding serious crime, including terrorism, child sexual abuse, and cybercrime, directly from tech companies based in the other country, without legal barriers" according to the DOJ's press release. The agreement was made under the mechanism put in place by the "Clarifying Lawful Overseas Use of Data Act" (the CLOUD Act), the statute Congress enacted to address the problems presented in the *United States v. Microsoft* case where the company refused to provide email stored on servers in Ireland to U.S. law enforcement agencies in a criminal investigation. Also, of note, the day before the agreement was announced, the U.S., U.K., and Australia sent Facebook an "open letter" regarding the company's March announcement that it would be "implementing end-to-end encryption for all private communications," asking that the company "not proceed with its plan...without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens."

It appears these governments are using the occasion of a new data sharing agreement to pressure Facebook in particular and the technology industry in general, but also this letter comes at a time when Facebook is under U.S. federal and state antitrust investigations following a $5 billion settlement with the FTC, EU investigations into antitrust and data security investigations and scrutiny because of its proposed Libra cryptocurrency.

Additionally, the U.S. and other members of the Five Eyes are reframing the issue of default end-to-end encryption in the context of pedophiles, sexual predators, and terrorism, grounds the nations likely believe are more favorable to their case that technology companies should develop means to defeat encryption when needed by law enforcement agencies. This pivot is evidenced by the messaging of the U.S. and UK governments:

> Attorney General William Barr said: "This agreement will enhance the ability of the United States and the United Kingdom *to fight serious crime -- including terrorism, transnational organized crime, and child exploitation* -- by allowing more efficient and effective access to data needed for quick-moving investigations. Only by addressing the problem of timely access to electronic evidence of crime committed in one country that is stored in another, can we hope to keep pace with twenty-first century threats. This agreement will make the citizens of both countries safer, while at the same time assuring robust protections for privacy and civil liberties."
> Home Secretary Priti Patel said: "*Terrorists and paedophiles continue to exploit the internet to spread their messages of hate, plan attacks on our citizens and target the most vulnerable*. As Home Secretary I am determined to do everything in my power to stop them. This historic agreement will dramatically speed up investigations, allowing our law enforcement agencies to protect the public. This is just one example of the enduring security partnership we have with the United States and I look forward to continuing to work with them and global partners to tackle these heinous crimes." (Emphasis added.)

According to a Home Ministry press release, the "UK-US Bilateral Data Access Agreement" will "dramatically speed up investigations and prosecutions by enabling law enforcement, with appropriate authorisation, to go directly to the tech companies to access data, rather than through governments, which can take years." The DOJ contended that the agreement "will dramatically speed up investigations by removing legal barriers to timely and effective collection of electronic evidence...[and] [u]nder its terms, law enforcement, when armed with appropriate court authorization, may go directly to tech companies based in the other country to access electronic data, rather than going through governments, which can take years."

The DOJ claimed in its press release that

> Both governments agreed to terms which broadly lift restrictions for a broad class of investigations, not targeting residents of the other country, and assure providers that disclosures through the Agreement are compatible with data protection laws. Each also committed to obtain permission from the other before using data gained through the agreement in prosecutions relating to a Party's essential interest—specifically, death penalty prosecutions by the United States and UK cases implicating freedom of speech.

The DOJ stated that "[t]he United States will have reciprocal access, under a U.S. court order, to data from UK communication service providers...[and] [a]ll requests for access to data will be subject to independent judicial authorization or oversight." The DOJ and the Home Ministry stated that they "anticipate releasing a copy of the agreement in the near future following Congressional and Parliamentary notification."

In terms of additional steps, under the CLOUD Act, the DOJ, in concurrence with the Department of State must now submit a written certification of its determination that UK meets a number of requirements, including "the domestic law of the foreign government, including the implementation

of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" among others. Additionally, DOJ Must certify its determination, in this case, that the UK "has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement." Notably, one of these determinations is that "the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data." Consequently, a CLOUD Act "executive agreement on access to data by a foreign government" cannot establish a duty for technology providers to decrypt data.

Congress must then consider whether to accept or reject this written determination. There are accelerated procedures for both the House and Senate to enact a joint resolution of disapproval of any certification with which it disagrees. If Congress does not pass such a resolution, the certification becomes operative in 90 days. Additionally, any such certification by DOJ may not be challenged in court or administratively.

Also of note regarding this agreement was the October 4 DOJ "Lawful Access Summit" with appearances by Barr, Deputy Attorney General Jeffrey Rosen, and FBI Director Christopher Wray, among others.

In a development related to the announcement of the UK-US Bilateral Data Access Agreement, Attorney General William Barr, Acting Secretary of Homeland Security Kevin McAleenan, U.K. Home Secretary Priti Patel, and Australia's Minister for Home Affairs Peter Dutton sent a letter to Facebook CEO Mark Zuckerberg "to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens." These officials referenced the communications their governments have had with the social media platform on this issue and noted "Facebook has not committed to address our serious concerns about the impact its proposals could have on protecting our most vulnerable citizens." Barr, McAleenan, Patel, and Dutton claimed "[w]e support strong encryption...[and] respect promises made by technology companies to protect users' data...[but] "[w]e must find a way to balance the need to secure data with public safety and the need for law enforcement to access the information they need to safeguard the public, investigate crimes, and prevent future criminal activity." The officials asserted that "[c]ompanies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes."

Barr, McAleenan, Patel, and Dutton called on Facebook to do the following:

- Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;
- Enable law enforcement to obtain lawful access to content in a readable and usable format;
- Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions; and
- Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational.

Of course, encryption experts have consistently said that such actions are ultimately incompatible and therefore not possible using current technology and methods. Moreover, this is not the first time

these three governments have called on technology companies to do this. This past summer, the Five Eyes intelligence alliance issued a communique in which it urged technology companies "to include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format." Interestingly, at that time, these nations lauded Facebook for "approaches like Mark Zuckerberg's public commitment to consulting Governments on Facebook's recent proposals to apply end-to-end encryption to its messaging services…[and] [t]hese engagements must be substantive and genuinely influence design decisions." It begs the question of what, if anything, has changed since this communique was issued and the recent letter to Zuckerberg. In any event, this communique followed the Five Eyes 2018 "Statement of Principles on Access to Evidence and Encryption," which articulated these nations' commitment to working with technology companies to address encryption and the need for law enforcement agencies to meet their public safety and protection obligations.

Finally, it bears note that the DOJ and Australia's Ministry for Home Affairs have announced talks to develop a similar agreement under the CLOUD Act. This could be the most significant CLOUD Act agreement given Australia's recently enacted "Telecommunications and Other Legislation (Assistance and Access) Act 2018," legislation that critics are claiming could allow Australia's government to force technology companies to decrypt information or provide backdoors to law enforcement. If these claims are true, then a CLOUD Act agreement between the U.S. and Australia could allow the U.S. government to leverage Australia's law to access communications that would otherwise be inaccessible under current U.S. law. And, this facet of the issue does not take into account the Five Eyes' intelligence sharing agreement and network between the US, UK, Australia, Canada, and New Zealand, which could theoretically be a conduit for data obtained by the Australian government to be disseminated to the other four nations. However, Australia has yet to enact an enabling statute that would allow its government to enter into such an agreement, and until such time no such agreement could be struck with the US.

DC Circuit Decision on Net Neutrality Opens Way For States

In a highly anticipated decision, the United States Court of Appeals for the District Of Columbia Circuit (D.C. Circuit) upheld most of the Federal Communications Commission's (FCC) repeal of the its earlier net neutrality rule (i.e. In re Restoring Internet Freedom, 33 FCC Rcd. 311 (2018)). However, the D.C. Circuit declined to accept the FCC"s attempt to preempt all contrary state laws and struck down this part of the FCC's rulemaking. Consequently, states and local jurisdictions may now be free to enact regulations of internet services along the lines of the FCC's now repealed Open Internet Order. The D.C. Circuit also sent the case back to the FCC for further consideration on three points.

The D.C. Circuit provided this background on the 2015 and 2018 orders, the former of which classified internet service providers (ISP) as common carriers under Title II of the Communications Act, and the latter of which reclassified ISPs as information services:

> The 2018 Order and today's litigation represent yet another iteration of a long-running debate regarding the regulation of the Internet. We rehearsed much of this complex history in *United States Telecom Association v. FCC*, 825 F.3d 674, 689–697 (D.C. Cir. 2016) ("USTA"), and see no need to recapitulate here what was so well and thoroughly said there. In the interest of reader-friendliness, though, we briefly review certain highlights necessary to understand this opinion.
>
> ….

> The 2018 Order accomplishes a number of objectives. First, and most importantly, it classifies broadband Internet as an "information service," *see 2018 Order* ¶¶26–64, and mobile broadband as a "private mobile service," *see id.* ¶¶ 65– 85. Second, relying on Section 257 of the Act (located in Title II but written so as to apply to Titles I through VI), the Commission adopts transparency rules intended to ensure that consumers have adequate data about Internet Service Providers' network practices. *See id.* ¶¶ 209–38. Third, the Commission undertakes a cost-benefit analysis, concluding that the benefits of a market-based, "light-touch" regime for Internet governance outweigh those of common carrier regulation under Title II, *see id.* ¶¶ 304–323, resting heavily on the combination of the transparency requirements imposed by the Commission under Section 257 with enforcement of existing antitrust and consumer protection laws, *see id.* ¶¶ 140– 154. The Commission likewise finds that the burdens of the Title II Order's conduct rules exceed their benefits. *See id.* ¶¶ 246–266.

The D.C. Circuit stated that "[w]e uphold the 2018 Order, with two exceptions:

> First, the Court concludes that the Commission has not shown legal authority to issue its Preemption Directive, which would have barred states from imposing any rule or requirement that the Commission "repealed or decided to refrain from imposing" in the Order or that is "more stringent" than the Order. 2018 Order ¶ 195. The Court accordingly vacates that portion of the Order.
>
> Second, we remand the Order to the agency on three discrete issues:
>
> (1) The Order failed to examine the implications of its decisions for public safety;
>
> (2) the Order does not sufficiently explain what reclassification will mean for regulation of pole attachments; and
>
> (3) the agency did not adequately address Petitioners' concerns about the effects of broadband reclassification on the Lifeline Program.

Regarding its overturning of the FCC's attempt to bar state action on net neutrality, in relevant part, the D.C. Circuit vacated "the portion of the 2018 Order that expressly preempts "any state or local requirements that are inconsistent with [its] deregulatory approach." The D.C. Circuit claimed that FCC "ignored binding precedent by failing to ground its sweeping Preemption Directive—which goes far beyond conflict preemption—in a lawful source of statutory authority." The D.C. Circuit noted that "[t]hat failure is fatal."

The D.C. Circuit further explains that

> The relevant portion of the Order provides that "regulation of broadband Internet access service should be governed principally by a uniform set of federal regulations," and not "by a patchwork that includes separate state and local requirements." In service of that goal, the 2018 Order expressly "preempt[s] any state or local measures that would effectively impose rules or requirements that we have repealed or decided to refrain from imposing in this order or that would impose more stringent requirements for any aspect of broadband service that we address in this order." In other words, the Preemption Directive invalidates all state and local laws that the Commission deems to "interfere with federal regulatory objectives" or that involve "any aspect of broadband service * * * address[ed]" in the Order. The Preemption Directive conveys more than a mere intent for the agency to preempt state laws in the future if they conflict with the 2018 Order.

California, Vermont, and Colorado have enacted net neutrality laws that have not been enforced pending the outcome of this case. Currently six states require entities wishing to contract with the state to meet net neutrality rules: Hawaii, Montana, New Jersey, New York, Rhode Island, and Vermont. A number of states have proposed or are implementing the regulation of net neutrality and ISPs by its public utility commissions.

CJEU Rules Against Facebook

In seeming contradiction of its recent decision in *Google v. CNIL*, the Court of Justice of the European Union (CJEU or Court) has ruled that European Union (EU) law allows EU nations to order platforms the host content like in Facebook in this case to remove illegal content or any identical or equivalent illegal content in the EU and possibly throughout the world. Of course, this ruling seems contrary to the ruling in the *Google v. CNIL* case, but it must be stressed that the Google case was interpreting a provision of the General Data Protection Regulation (GDPR). This case interprets an older provision of EU law, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (aka the "Directive on electronic commerce.") Consequently, under this EU law, EU nations may enact and enforce laws to allow their courts to order multi-national platforms to remove unlawful information, copies of such information, and equivalent information. The CJEU added that an EU nation could also order "a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law." However, the CJEU stops short of imposing a duty on a company to conduct a comprehensive and exhaustive search on its platforms for all such illegal information; rather just that information deemed to be identical or equivalent would need to be taken down.

This case concerns "a message [on Facebook] containing statements harmful to the reputation of Ms Glawischnig-Piesczek...a member of the Nationalrat (National Council, Austria), chair of the parliamentary party 'die Grünen' (The Greens) and federal spokesperson for that party." The CJEU explained that

> On 3 April 2016, a Facebook Service user shared on that user's personal page an article from the Austrian online news magazine oe24.at entitled 'Greens: Minimum income for refugees should stay', which had the effect of generating on that page a 'thumbnail' of the original site, containing the title and a brief summary of the article, and a photograph of Ms Glawischnig-Piesczek. That user also published, in connection with that article, a comment which the referring court found to be harmful to the reputation of the applicant in the main proceedings, and which insulted and defamed her. This post could be accessed by any Facebook user.

The CJEU related that "[b]ecause Facebook Ireland did not withdraw the comment in question, Ms Glawischnig-Piesczek brought an action" that eventually reached Austria's Supreme Court (the Oberster Gerichtshof) which subsequently asked the CJEU for a preliminary ruling on EU law, specifically:

(1) Does Article 15(1) of Directive [2000/31] generally preclude any of the obligations listed below of a host provider which has not expeditiously removed illegal information, specifically not just this illegal information within the meaning of Article 14(1)(a) of [that] directive, but also other identically worded items of information:
   - worldwide;
   - in the relevant Member State;

- of the relevant user worldwide;
- of the relevant user in the relevant Member State?

(2) In so far as Question 1 is answered in the negative: does this also apply in each case for information with an equivalent meaning?

(3) Does this also apply for information with an equivalent meaning as soon as the operator has become aware of this circumstance?

As noted this case explicates a provision of EU law and regulation aside and apart from the GDPR. The CJEU explained that in substantive part, Article 15 of Directive [2000/31] provides that "[m]ember States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, (i.e. "mere conduit," "caching," and "hosting") to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

The CJEU held that

> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:
>
> - ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;
> - ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, and
> - ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

There are some important differences to note between the Facebook and Google decisions. First, the grounds upon which the challenges were brought differ. In the Google case, the CJEU was looking at the so-called Right To Be Forgotten under the GDPR, and in the Facebook case, the Court, as noted, was examining the applicability of Directive [2000/31]. Second, the information in Facebook was found to be defamatory and hence illegal while in the Google case, the French data protection authority (DPA) was acting generally when it informed 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 objected to this statement of policy and then was fined. Finally, the CJEU made clear in Google that while "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." The Court added that "[a]ccordingly, 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."

FDA Medical Device Cybersecurity Warnings

The U.S. Food and Drug Administration (FDA) released a warning that a commonly used third-party software component may contain a vulnerability that places certain medical devices at risk. The FDA informed "patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks" even though the agency "is not aware of any confirmed adverse events related to these vulnerabilities." The FDA noted that "software to exploit these vulnerabilities is already publicly available." This warning follows a June notice about cybersecurity concerns posed by an insulin pump.

The FDA stated that it "is working closely with other federal agencies, manufacturers, and security researchers to identify, communicate and prevent adverse events related to the URGENT/11 vulnerabilities…[and] will keep the public informed if significant new information becomes available.

In statements, two FDA officials provided additional detail. The FDA's Office of Strategic Partnerships and Technology Innovation Deputy Director Suzanne Schwartz stated that the "risk of patient harm if such a vulnerability were left unaddressed could be significant." She asserted that "[i]t's important for manufacturers to be aware that the nature of these vulnerabilities allows the attack to occur undetected and without user interaction…[and] [b]ecause an attack may be interpreted by the device as a normal network communication, it may remain invisible to security measures." The FDA's Principal Deputy Commissioner Amy Abernathy said the agency "urges manufacturers everywhere to remain vigilant about their medical products—to monitor and assess cybersecurity vulnerability risks, and to be proactive about disclosing vulnerabilities and mitigations to address them."

The FDA explained

> A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.
> These vulnerabilities exist in IPnet, a third-party software component that supports network communications between computers. Though the IPnet software may no longer be supported by the original software vendor, some manufacturers have a license that allows them to continue to use it without support. Therefore, the software may be incorporated into other software applications, equipment, and systems which may be used in a variety of medical and industrial devices that are still in use today.

The FDA stated that "[s]ecurity researchers, medical device manufacturers, and the FDA are aware

that some versions of the following operating systems are affected…[and]..the vulnerable IPnet software component may not be included in all versions of these operating systems:

- VxWorks (by Wind River)
- Operating System Embedded (OSE) (by ENEA)
- INTEGRITY (by Green Hills)
- ThreadX (by Microsoft)
- ITRON (by TRON Forum)
- ZebOS (by IP Infusion)

The FDA made the following recommendations to manufacturers:

- Conduct a risk assessment, as described in FDA's cybersecurity postmarket guidance, to evaluate the impact of these vulnerabilities to your medical device portfolio and develop risk mitigation plans. Please keep in mind that the nature of the vulnerabilities allows the attack to occur undetected and without user interaction. Because an attack may be interpreted by the affected device as normal and benign network communications, it may remain invisible to existing security measures.
- Work with the operating system vendor to identify if a patch is available and implement recommended mitigation methods. Medical device manufacturers will need to evaluate and validate the patch for their devices.
- Ensure any mitigations you may currently employ (for example: firewalls, virtual private network (VPN)) are not impacted by URGENT/11.
- Develop a plan for updating your medical device to accommodate a version of an OS (or a communication protocol) that is not impacted by the URGENT/11 vulnerabilities.
- Work with health care providers and facilities to determine affected medical devices and discuss and develop ways to ensure that risks are reduced to acceptable levels.
- Communicate with your customers and the user community regarding your assessment and recommendations for risk mitigation strategies and any compensating controls, to allow customers to make informed decisions about device use. Provide an Information Sharing Analysis Organization (ISAO) with any customer communications upon notification of your customers.
- Report medical devices you've identified as vulnerable to URGENT/11 to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) at ICS-CERT@HQ.DHS.GOV, so that this information can be added to its evolving list of products.

Further Reading

- "Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight." – *The New York Times*. As we have periodically informed you, stakeholders in Congress are not close to reaching agreement on a privacy bill even with the effective date of the CCPA looming. Now it remains to be seen whether federal privacy legislation like federal data security and breach notification fades in the event industry decides they can live with the CCPA and similar statutes. Nonetheless, this article claims that Senators Jerry Moran (R-KS) and Richard Blumenthal (D-CT) may be close to releasing a bill, and so is the House Energy and Commerce Committee.
- "U.S. online privacy rules unlikely this year, hurting big tech" – *Reuters*. This article on the state of play for privacy legislation in Congress predicts a best case scenario as the release of a discussion draft before year's end. However, fault lines continue to be whether an enhanced notice and consent regime would satisfy stakeholders and the extent to which consumer information can be shared with third parties. This article also alleges that Moran

and Blumenthal and the House Energy and Commerce Committee release bills in the near future.

- "NSA launches new cyber defense directorate" – *The Washington Post*. The National Security Agency unveiled its long rumored new Cybersecurity Directorate, "a major organization that unifies NSA's foreign intelligence and cyberdefense missions" according to an NSA press release. The new entity will share better cyber threat information with private sector entities in critical sectors. Critics claim a reorganization was not necessary, and the NSA could have emphasized this mission through its Information Assurance Directorate.
- "With Facebook's Coming News Tab, Only Some Will Get Paid" – *The Wall Street Journal*. Contrary to what some might have hoped for in the journalism industry, the social media platform will not be contributing to many organizations cash flow that appear on the new News feature. Facebook is looking to strike three year deals that could pay $3 million a year to organizations like the Wall Street Journal and less for regional publications. Facebook is also trying to avoid further conservative ire by working to include some conservative media sources while still trying to screen out disreputable sources regardless of political orientation.
- "Inside Pioneer: May the Best Silicon Valley Hustler Win" – *WIRED*. A tale that could only come from Silicon Valley. Startup entrepreneurs playing a game in the style of the Hunger Games without the killing.
- "Silicon Valley donors starting to back Elizabeth Warren despite her pledge to break up Big Tech" – *CNBC*. Even though she is refusing to do the kind of big money events at which Silicon Valley gets to access candidates and she wants to break up the tech giants, Senator Elizabeth (D-WA) is increasingly the front runner among many in the tech industry for a variety of reasons: her rivals seem to be dropping by the wayside, it seems like she can beat the President, and the realities of how changes happens or does not in Washington may be tempering fear about a Warren Administration.
- "Amazon sellers say online retail giant is trying to help itself, not consumers" – *Washington Post*. Turns out that Amazon is charging more and more fees and imposing more costs on the vendors that sell on its platform. Apparently, vendors have to pay $5,000 a month just reach a person or get support from the website, and vendors are paying to appear at the top of search results. At the same time, Amazon is rolling out more and more of its own branded products. Nonetheless as much as .35 cents of each dollar a vendor earns on Amazon goes to the tech giant.
- "Big Tech's Complexity Will Strain FTC Resources, Agency Warns" – *Bloomberg*. The Federal Trade Commission's Inspector General identified the increasingly complex, possibly increasingly expensive nature of investigations into technology firms being among the FTC's top challenges.
- "Fighting Cyber Crime is Critical for National Security, Says Secret Service Chief" – *Nextgov*. The agency responsible for policing cyber crime makes the case for including transnational cyber criminals in the U.S.'s whole-of-government response on nation-state challenges.