Technology Policy Update
28 February 2020
By Michael Kans, Esq.

Agency Heads Explain U.S. Efforts To Fend Off Election Interference

In an opinion piece, Attorney General William Barr, Federal Bureau of Investigation Director Christopher Wray, outgoing acting Director of National Intelligence Joseph Maguire, acting Secretary of Homeland Security Chad Wolf and Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs addressed concerns about election interference in the 2020 primaries and general election, discussed federal and state efforts, and sought to assure the American public that, to date, the efforts of other nations have not had a material effect on elections. Additionally these officials discussed foreign interference in broad strokes without confirming or denying Russian efforts to assist the Trump campaign in the 2016 election.

Like many previous statements, Barr, Wray, Maguire, Wolf, and Krebs continue to emphasize that the election interference to worry about is changing vote tallies or prevent voting instead of the disinformation campaign waged by Russia in the last election. Consequently, by these metrics, the officials were able to claim there has been no interference to date. Barr, Wray, Maguire, Wolf, and Krebs claimed that "[w]e have yet to identify any activity designed to prevent voting or change votes…[but] we remain watchful of any malicious activities from cybercriminals and from foreign actors like Russia, China and Iran."

They further claimed that

- The states' autonomy over elections makes our elections more resilient. The diversity of election systems among the states, multiple checks and redundancies in those systems, and post-election auditing all make it extraordinarily difficult for foreign adversaries to disrupt or change vote tallies.
- States have plans in place, like provisional ballots, to enable a reliable election to proceed in the case that interference does occur. While the states have primary responsibility for administering elections under our Constitution, our agencies continue to provide them with support by identifying best practices for voting systems, sharing threat information and offering services and resources.

These arguments are made despite significant evidence that a number of states and their systems are not secure against cyberattacks.

Barr, Wray, Maguire, Wolf, and Krebs stated that "[s]everal of our agencies are working directly with campaigns and candidates to educate them about ways to help keep their networks secure…[and] [w]e are mobilized and working with states to identify cybersecurity threats to their own systems and to campaigns, and we are better able to warn them about threats today than ever before." They said that "[y]ou can play an important role, too:

- First, you can participate in the process. All Americans should be undeterred by concerns of attempted foreign interference and have full confidence that a vote cast is a vote counted. The best way to understand how your elections are secured is to engage with your state and local officials, or to volunteer to serve as a poll worker and help support the election

process yourself. Don't fall prey to disinformation about your election — such as when, where or how to vote — from untrusted sources. State and local government websites are the authoritative sources for this information.

- Second, we encourage candidates, election officials, technology companies and others involved in elections to report suspicious cyber activity to us. The FBI and the Cybersecurity and Infrastructure Security Agency have set up election-focused websites that host additional information about election security and provide avenues to report concerns.
- Third, an informed and discerning public is a resilient public. As consumers of all types of media, you can help separate facts from falsehoods by seeking trustworthy sources for information and by evaluating what you read or watch with a critical eye. Some foreign governments have a track record of meddling in our affairs by attempting to shape public opinion and voter perceptions. Foreign actors have done this by hacking and dumping private campaign and candidate information on the internet and spreading disinformation and divisive messages on social media.

Barr, Wray, Maguire, Wolf, and Krebs added

- Often, we see foreign adversaries amplifying messages some Americans create and share with each other, in an effort to stoke hostility among us and make us appear more divided than we are. They seek to undermine our trust and confidence in each other, our democratic society and democracy itself.
- To combat this threat, we continue to strengthen partnerships with technology and social media companies and share more information than ever before. Those companies are taking more responsibility for preventing foreign adversaries from weaponizing their platforms. Additionally, we must remain aware that foreign adversaries continue to spread disinformation to discredit politicians and views that are counter to their interests and ambitions.
- We cannot prevent all disinformation, foreign propaganda or cyberattacks on our infrastructure. However, together, we can all help to mitigate these threats by exercising care when we share information and by maintaining good cyber hygiene to reduce the risks that malicious cyberattacks will succeed.

EC Unveils Digital Strategy, Data Strategy, and AI White Paper

The European Commission (EC) has released a digital strategy, Shaping Europe's Digital Future, along with two components of this strategy: a "European strategy for data" and a white paper on artificial intelligence. This initiative flows from the new European leadership and could significantly change how the European Union (EU) regulates technology and data in the future. However, much of the digital strategy hinges on yet to be developed regulatory and legislative initiatives, so how it is actually implemented remains to be seen. Nonetheless, given how the EU's General Data Protection Regulation (GDPR) changed how privacy and personal data have been seen and regulated inside and outside of the U.S., the EU's digital strategy bears watching as the Europeans seem intent on charting a course on technology independent of the U.S. and China.

Digital Strategy

The EC explained "[i]n her political guidelines, [new EC] President [Ursula] von der Leyen stressed the need for Europe to lead the transition to a healthy planet and a new digital world." The EC stated that over the next five years, it "will focus on three key objectives to ensure that digital

solutions help Europe to pursue its own way towards a digital transformation that works for the benefit of people through respecting our values...[and] will also put Europe in a position to be a trendsetter in the global debate:

- Technology that works for people: Development, deployment and uptake of technology that makes a real difference to people's daily lives. A strong and competitive economy that masters and shapes technology in a way that respects European values.
- A fair and competitive economy: A frictionless single market, where companies of all sizes and in any sector can compete on equal terms, and can develop, market and use digital technologies, products and services at a scale that boosts their productivity and global competitiveness, and consumers can be con dent that their rights are respected.
- An open, democratic and sustainable society: A trustworthy environment in which citizens are empowered in how they act and interact, and of the data they provide both online and offline. A European way to digital transformation which enhances our democratic values, respects our fundamental rights, and contributes to a sustainable, climate-neutral and resource-efficient economy.

The EC claimed that "[f]or Europe to truly influence the way in which digital solutions are developed and used on a global scale, it needs to be a strong, independent and purposeful digital player in its own right." The EC asserted that "[i]n order to achieve this, a clear framework that promotes trustworthy, digitally enabled interactions across society, for people as well as for businesses, is needed...[and] [w]ithout this focus on trustworthiness, the vital process of digital transformation cannot succeed."

The EC listed a number of "Key Actions" the EU is already engaged in or wioll engage in to bring about this Digital Strategy, including but not limited to:

- White Paper on Artificial Intelligence setting out options for a legislative framework for trustworthy AI (adopted together with this Communication), with a follow-up on safety, liability, fundamental rights and data (Q4 2020).
- Building and deploying cutting-edge joint digital capacities in the areas of AI, cyber, super- and quantum computing, quantum communication and blockchain. European Strategies on Quantum and blockchain (Q2 2020) as well as a revised EuroHPC Regulation on supercomputing.
- Accelerating investments in Europe's Gigabit connectivity, through a revision of the Broadband Cost Reduction Directive, an updated Action Plan on 5G and 6G, a new Radio Spectrum Policy Programme (2021). 5G corridors for connected and automated mobility, including railway corridors, will be rolled out (2021-2030) (2021-2023).
- A European cybersecurity strategy, including the establishment of a joint Cybersecurity Unit, a Review of the Security of Network and Information Systems (NIS) Directive and giving a push to the single market for cybersecurity.
- Initiative to improve labour conditions of platform workers (2021).
- A reinforced EU governments interoperability strategy to ensure coordination and common standards for secure and borderless public sector data flows and services. (2021)
- A European Data Strategy to make Europe a global leader in the data-agile economy (February 2020), announcing a legislative framework for data governance (Q4 2020) and a possible Data Act (2021).
- Ongoing evaluation and review of the fitness of EU competition rules for the digital age (2020-2023), and launch of a sector inquiry (2020).

- Create a framework to enable convenient, competitive and secure Digital Finance, including legislative proposals on crypto assets, and on digital operational and cyber resilience in the financial sector and a strategy towards an integrated EU payments market that supports pan-European digital payment services and solutions (Q3 2020);
- Communication on Business Taxation for the 21st century, taking into account the progress made in the context of the Organisation for Economic Co-operation and Development (OECD) to address the tax challenges arising from the digitisation of the economy.
- Delivering a new Consumer Agenda, which will empower consumers to make informed choices and play an active role in the digital transformation (Q4 2020).
- • New and revised rules to deepen the Internal Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforce the oversight over platforms' content policies in the EU. (Q4 2020, as part of the Digital Services Act package).
- European Democracy Action Plan to improve the resilience of our democratic systems, support media pluralism and address the threats of external intervention in European elections (Q4 2020)
- A Global Digital Cooperation Strategy (2021).
- A White Paper on an instrument on foreign subsidies (Q2 2020).
- A strategy for standardisation, which will allow for the deployment of interoperable technologies respecting Europe's rules, and promote Europe's approach and interests on the global stage (Q3 2020).

European Data Strategy

The EC asserted that the "EU can become a leading role model for a society empowered by data to make better decisions – in business and the public sector...[and] [t]o fulfill this ambition, the EU can build on a strong legal framework – in terms of data protection, fundamental rights, safety and cybersecurity – and its internal market with competitive companies of all sizes and varied industrial base." The EC claimed that "[i]f the EU is to acquire a leading role in the data economy, it has to act now and tackle, in a concerted manner, issues ranging from connectivity to processing and storage of data, computing power and cybersecurity. Moreover, it will have to improve its governance structures for handling data and to increase its pools of quality data available for use and re-use."

The EC stated that "[t]he measures laid out in this paper contribute to a comprehensive approach to the data economy that aim to increase the use of, and demand for, data and data-enabled products and services throughout the Single Market...[and] outlines a strategy for policy measures and investments to enable the data economy for the coming five years." The EC explained this strategy will launch "a comprehensive consultation on the specific measures that could be taken to keep the EU at the forefront of the data-agile economy, while respecting and promoting the fundamental values that are the foundation of European societies."

The European Data Strategy is "based on four pillars," and the EC has identified a number of key actions to realize the strategy:

> *A. A cross-sectoral governance framework for data access and use*
> Cross-sectoral (or horizontal) measures for data access and use should create the necessary over-arching framework for the data-agile economy, thereby avoiding harmful fragmentation of the internal market through inconsistent actions between sectors and

between the Member States. Such measures should nonetheless take into account the specificities of individual sectors and of the Member States.

Key actions

- Propose a legislative framework for the governance of common European data spaces, Q4 2020
- Adopt an implementing act on high-value data-sets, Q1 2021
- Propose, as appropriate, a Data Act, 2021
- Analysis of the importance of data in the digital economy (e.g. through the Observatory of the Online Platform Economy), and review of the existing policy framework in the context of the Digital Services Act package (Q4 2020).

B. Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability

Europe's data strategy relies on a thriving ecosystem of private actors to create economic and societal value from data. Start-ups and scale-ups will play a key role in developing and growing disruptive new business models that fully take advantage of the data revolution. Europe should offer an environment that supports data-driven innovation and stimulates demand for products and services that rely on data as an important factor of production.

Key actions

- Invest in a High Impact project on European data spaces, encompassing data sharing architectures (including standards for data sharing, best practices, tools) and governance mechanisms, as well as the European federation of energy-efficient and trustworthy cloud infrastructures and related services, with a view to facilitating combined investments of €4-6 billion, of which the Commission could aim at investing €2 billion. First implementation phase foreseen for 2022;
- Sign Memoranda of Understanding with Member States on cloud federation, Q3 2020;
- Launch a European cloud services marketplace, integrating the full stack of cloud service offering, Q4 2022;
- Create an EU (self-)regulatory cloud rulebook, Q2 2022.

C. Competences: Empowering individuals, investing in skills and in SMEs

Key action

- Explore enhancing the portability right for individuals under Article 20 of the GDPR giving them more control over who can access and use machine-generated data (possibly as part of the Data Act in 2021).

D. Common European data spaces in strategic sectors and domains of public interest

In complement to the horizontal framework, as well as to the funding and the actions on skills and empowerment of individuals under A, B and C, the Commission will promote the development of common European data spaces in strategic economic sectors and domains of public interest. These sectors or domains are those where the use of data will have systemic impact on the entire ecosystem, but also on citizens.

Key action

- Create a framework to measure data flows and estimate their economic value within Europe, as well as between Europe and the rest of the world, Q4 2021.

AI White Paper

The EC released the latest policy pronouncement on artificial intelligence, "On Artificial Intelligence - A European approach to excellence and trust," in which the Commission articulates its support for "a regulatory and investment oriented approach with the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of this new technology." The EC stated that "[t]he purpose of this White Paper is to set out policy options on how to achieve these objectives...[but] does not address the development and use of AI for military purposes." The EC is accepting comments until May 19, 2020, most of which will be made public. The EC explained that the "main building blocks of this White Paper are:

- The policy framework setting out measures to align efforts at European, national and regional level. In partnership between the private and the public sector, the aim of the framework is to mobilise resources to achieve an 'ecosystem of excellence' along the entire value chain, starting in research and innovation, and to create the right incentives to accelerate the adoption of solutions based on AI, including by small and medium-sized enterprises (SMEs).
- The key elements of a future regulatory framework for AI in Europe that will create a unique 'ecosystem of trust'. To do so, it must ensure compliance with EU rules, including the rules protecting fundamental rights and consumers' rights, in particular for AI systems operated in the EU that pose a high risk. Building an ecosystem of trust is a policy objective in itself, and should give citizens the confidence to take up AI applications and give companies and public organisations the legal certainty to innovate using AI. The Commission strongly supports a human-centric approach based on the Communication on Building Trust in Human-Centric AI8 and will also take into account the input obtained during the piloting phase of the Ethics Guidelines prepared by the High-Level Expert Group on AI.

In conjunction with the release of the white paper, the EC issued a "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics" that assesses the legal backdrop of the EU visa vis AI and could serve to inform and guide legislative changes to regulate AI.

FTC Demands Ten Years of Information From Big Tech On Mergers and Acquisitions

The Federal Trade Commission (FTC) has issued an order to a number of large technology companies with an eye towards determining if the current threshold for federal examination of mergers and acquisitions is too high for a number of technology-related acquisitions. However, larger acquisitions above the threshold of about $90 million are not part of this examination such as Facebook's $22 billion purchase of WhatsApp. Agency officials were also quoted as saying that the inquiry is bigger than anti-competitive issues as there may be ulterior motives for the rash of acquisitions in this sector. Moreover, this order was issued at a time when the agency, the Department of Justice (DOJ), state attorneys general, and the House Judiciary Committee are examining antitrust and anti-competitive practices in the technology world.

Nonetheless, the agency is asking that major technology firms turn over information on mergers and acquisitions that were too small for the FTC or the DOJ to investigate potential anti-competitive effects. And, while the information gleaned from such an inquiry may not be used for an investigation that could result in legal action, the FTC may do so under the FTC Act if it so chooses.

In a conference call with reporters, FTC Chair Joe Simons remarked "[i]f during this study we see that there are transactions that turn out were problematic, all of our options are on the table."

The FTC sent letters to Alphabet, Amazon, Apple, Facebook, and Microsoft "to provide information and documents on the terms, scope, structure, and purpose of transactions that each company consummated between Jan. 1, 2010 and Dec. 31, 2019" according to the agency's press release.

In an FAQ, the FTC stated

> We plan to use the responses to our Special Orders to better understand acquisitions by certain technology companies. In particular, the study will help the FTC assess whether U.S. antitrust authorities are receiving adequate notice of transactions that might limit or eliminate competition. The Hart-Scott-Rodino (HSR) Antitrust Improvements Act requires premerger filings when the parties and the transaction meet certain size thresholds. The FTC will study whether large tech companies are making potentially anticompetitive acquisitions—including acquisitions of nascent or potential competitors—that fall below HSR filing thresholds.

The FTC explained that these orders are issued "under Section 6(b) of the FTC Act, which authorizes the Commission to conduct wide-ranging studies that do not have a specific law enforcement purpose." The agency claimed that "[t]he orders will help the FTC deepen its understanding of large technology firms' acquisition activity, including how these firms report their transactions to the federal antitrust agencies, and whether large tech companies are making potentially anticompetitive acquisitions of nascent or potential competitors that fall below HSR filing thresholds and therefore do not need to be reported to the antitrust agencies."

The FTC added

- The Special Orders require each recipient to identify acquisitions that were not reported to the FTC and the U.S. Department of Justice under the HSR Act, and to provide information similar to that requested on the HSR notification and report form. The orders also require companies to provide information and documents on their corporate acquisition strategies, voting and board appointment agreements, agreements to hire key personnel from other companies, and post-employment covenants not to compete. Last, the orders ask for information related to post-acquisition product development and pricing, including whether and how acquired assets were integrated and how acquired data has been treated.
- The Commission plans to use the information obtained in this study to examine trends in acquisitions and the structure of deals, including whether acquisitions not subject to HSR notification might have raised competitive concerns, and the nature and extent of other agreements that may restrict competition. The Commission also seeks to learn more about how small firms perform after they are acquired by large technology firms. These and related issues were discussed during several sessions of the FTC's 2018 Hearings on Competition and Consumer Protection in the 21st Century, and this study is part of the follow-up from those Hearings.

Simons stated that "[t]his initiative will enable the Commission to take a closer look at acquisitions in this important sector, and also to evaluate whether the federal agencies are getting adequate notice of transactions that might harm competition…[and] will help us continue to keep tech markets open and competitive, for the benefit of consumers."

In a tweet, Commissioner Rohit Chopra suggested the FTC may be interested in more than just anti-competitive mergers.

> Companies across the economy are in an arms race to soak up every source of data and monetize it. Many of these mergers fly below the radar. The FTC orders will provide clarity on why boardrooms are shelling out billions for our personal data.

As noted, the FTC and DOJ are in the midst of investigations into big technology companies. However, the agencies had supposedly divided the investigation with the FTC looking at Facebook and Amazon and the DOJ investigating Google and Apple. However, there have been reports that the DOJ and the FTC have been fighting over who is investigating whom with the FTC and DOJ confirming a dispute in testimony before the Senate Judiciary Committee last fall.

The House Judiciary Committee's Antitrust, Commercial, and Administrative Law Subcommittee held its fifth hearing on competition in digital markets in January and is expected to at least issue a report and possibly even legislative language to reform the antitrust and anti-competitive statutory and regulatory landscape.

Additionally, New York Attorney General Letitia James is leading an antitrust investigation of Facebook that almost all state attorneys general are part of while Texas Attorney General Ken Paxton is leading almost all state attorneys general's investigation of Google for possible antitrust violations.

Finally, Senators Bernie Sanders (I-VT) and Elizabeth Warren (D-MA) have called for the breakup of large technology companies as part of their campaigns to secure the Democratic nomination for president.

Estonian Foreign Intelligence Service Continues To Detail Russian Threat

The Estonian Foreign Intelligence Service (Välisluureamet) released its annual report titled "International Security and Estonia," and again the nation devoted the bulk of the report to Russian activities conducted throughout the whole of Europe to expand their influence and disrupt the efforts of Western nations. Not surprisingly, Estonia focused on cyber and information operations given their widespread use through the region by Russian hackers. The report was released days before the United States, United Kingdom, Australia, the Netherlands, Romania, Poland, and other nations claimed Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies had conducted widespread offensive cyber operations in Georgia in October 2019. However, Estonia also included sections detailing the threats posed by China in the technology sphere.

Regarding Russia, Välisluureamet stated

- Cyber operations are an effective means for Russia to achieve its political goals They are affordable in terms of people, time and financial resources, and allow Russia to operate below the threshold of armed conflict The targets of Russian cyber operations have changed little through the years – the target countries are mostly the same, while the range of targeted sectors has expanded over time The strategic objectives of the operations –

projecting the image of a superpower and maintaining internal stability – also remain unchanged What changes, however, is the methods used to perform the cyber operations, which is why consistent enhancement of cyber security is crucial.

- Russia's cyber operations have been successful and, to date, have not been sanctioned enough by the West to force Russia to abandon them As Russia has received the signal that cyber operations are justifying themselves, these operations will continue to be a security threat, to Estonia among others.
- In 2019, Russian cyber operations were revealed that have been going on undiscovered for years, and there are likely to be more In addition to their continuity, Russia's cyber operations are characterised by the tendency to exploit situations as they arise – as security vulnerabilities become public, the Russians are eager to exploit these immediately against their existing targets For example, only a month after a security vulnerability was announced in February 2019, Russian cyber actors attempted to exploit it in an operation against an international organisation This case demonstrates again how important it is to constantly update the so ware of your IT systems.

Regarding China, Välisluureamet claimed:

- The threat of Chinese technology is strategic and will be revealed in the long term China has a different culture and values than the West and a repressive communist regime in power As one aspect of building its global influence, China creates dependencies in other countries step by step, over the long term.
- For a digital nation like Estonia, communications networks are a vital piece of infrastructure, and all the risks associated with the technology used need to be considered Small countries are an easier target for China to build dependency and exert pressure later.

FCC Seeks Comment On Three Issues Sent Back to Commission in Mozilla Decision

After losing in federal court, the Federal Communications Commission (FCC) is seeking comment on the issues the court found did not pass muster in the FCC's rollback of net neutrality, "Restoring Internet Freedom Order."

In 2014, the U.S. Court of Appeals for the District of Columbia struck down a 2010 FCC net neutrality order in *Verizon v. FCC*, but the court did suggest a path forward. The court held the FCC "reasonably interpreted section 706 to empower it to promulgate rules governing broadband providers' treatment of Internet traffic, and its justification for the specific rules at issue here—that they will preserve and facilitate the "virtuous circle" of innovation that has driven the explosive growth of the Internet—is reasonable and supported by substantial evidence." The court added that "even though the Commission has general authority to regulate in this arena, it may not impose requirements that contravene express statutory mandates...[and] [g]iven that the Commission has chosen to classify broadband providers in a manner that exempts them from treatment as common carriers, the Communications Act expressly prohibits the Commission from nonetheless regulating them as such." However, in 2016, the same court upheld the 2015 net neutrality regulations in *U.S. Telecom Association v. FCC,* and then upheld most of the FCC's repeal of the its earlier net neutrality rule. 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.

In the notice soliciting comments on the outstanding legal issues the FCC must reconsider, the Commission stated

> In the *Restoring Internet Freedom Order*, the Commission ended utility-style regulation of the Internet and returned to the light-touch framework under which a free and open Internet underwent rapid and unprecedented growth for almost two decades. In *Mozilla Corp. v. FCC*, the U.S. Court of Appeals for the District of Columbia Circuit upheld the vast majority of the Commission's decision, remanding three discrete issues for further consideration by the Commission. On February 6, 2020, the D.C. Circuit denied all pending petitions for rehearing, and the Court issued its mandate on February 18, 2020. With this Public Notice, the Wireline Competition Bureau seeks to refresh the record regarding the issues remanded to the Commission by the *Mozilla* Court.

The FCC listed the issues on which it wants comment:

- *Public Safety*. First, we seek to refresh the record on how the changes adopted in the *Restoring Internet Freedom Order* might affect public safety. In the *Restoring Internet Freedom Order*, the Commission predicted, for example, that permitting paid prioritization arrangements would "increase network innovation," "lead[] to higher investment in broadband capacity as well as greater innovation on the edge provider side of the market," and "likely . . . be used to deliver enhanced service for applications that need QoS [i.e., quality of service] guarantees." Could the network improvements made possible by prioritization arrangements benefit public safety applications—for example, by enabling the more rapid, reliable transmission of public safety-related communications during emergencies?
- *Pole Attachments*. Second, we seek to refresh the record on how the changes adopted in the *Restoring Internet Freedom Order* might affect the regulation of pole attachments in states subject to federal regulation. To what extent are ISPs' pole attachments subject to Commission authority in non-reverse preemption states by virtue of the ISPs' provision of cable or telecommunications services covered by section 224? What impact would the inapplicability of section 224 to broadband-only providers have on their access to poles? Have pole owners, following the *Order*, "increase[d] pole attachment rates or inhibit[ed] broadband providers from attaching equipment"? How could we use metrics like increases or decreases in broadband deployment to measure the impact the *Order* has had on pole attachment practices? Are there any other impacts on the regulation of pole attachments from the changes adopted in the *Order*? Finally, how do any potential considerations about pole attachments bear on the Commission's underlying decision to classify broadband as a Title I information service?
- *Lifeline Program*. Third, we seek to refresh the record on how the changes adopted in the *Restoring Internet Freedom Order* might affect the Lifeline program. In particular, we seek to refresh the record on the Commission's authority to direct Lifeline support to eligible telecommunications carriers (ETCs) providing broadband service to qualifying low-income consumers. In the *2017 Lifeline NPRM*, the Commission proposed that it "has authority under Section 254(e) of the Act to provide Lifeline support to ETCs that provide broadband service over facilities-based broadband-capable networks that support voice service," and that "[t]his legal authority does not depend on the regulatory classification of broadband

Internet access service and, thus, ensures the Lifeline program has a role in closing the digital divide regardless of the regulatory classification of broadband service." How, if at all, does the *Mozilla* decision bear on that proposal, and should the Commission proceed to adopt it?

Federal Court Approves T-Mobile/Sprint Merger; States May Appeal

Earlier this month, a United States District Court ruled in favor on the proposed merger between the third and fourth largest cellphone carriers in the United States, clearing the way for increased consolidation in that part of the telecommunications sector. Last year, the Trump Administration had thrown their support behind the T-Mobile/Sprint merger, but a number of state attorneys general challenged the proposed deal in federal court. It remains to be seen whether the decision will be challenged, especially since some of the state attorneys general have indicated they will accept the decision. However, this merger would seem to run contrary to the prevailing winds in Washington that nominally oppose greater tech sector consolidation. However, DISH Network's commitment to buying some of the two carriers prepaid plans and to build out its own 5G network were relied upon by the court and the Administration to allay concerns about decreased competition that could harm consumers.

In *New York v. Deutsche Telekom*, the U.S. District Court for Southern District of New York denied the states' challenge and request that the deal be blocked. However, the court conceded that in other markets, the states would have had a strong case for winning and injunction, but the court found that competition will not be substantially decreased as a result of the merger.

Here is the court's conclusion:

- Having been tasked with predicting the future state of the national and local retail mobile wireless telecommunications services (RMWTS) Markets both with and without the national and local RMWTS Markets both with and without the merger, and relying on both the evidence at trial and the various judicial tools available, the Court concluded that the Proposed Merger is not reasonably likely to substantially lessen competition in the RMWTS Markets. Despite the strength of Plaintiff States' prima facie case, which might well suffice to warrant injunction of mergers in more traditional industries, a variety of considerations raised at trial have persuaded the Court that a presumption of anticompetitive effects would be misleading in this particularly dynamic and rapidly changing industry. T-Mobile has redefined itself over the past decade as a maverick that has spurred the two largest players in its industry to make numerous pro-consumer changes. The Proposed Merger would allow the merged company to continue T-Mobile's undeniably successful business strategy for the foreseeable future.
- While Sprint has made valiant attempts to stay competitive in a rapidly developing and capital-intensive market, the overwhelming view both within Sprint and in the wider industry is that Sprint is falling farther and farther short of the targets it must hit to remain relevant as a significant competitor. Finally, the Federal Communications Commission (FCC) and Department of Justice (DOJ) have closely scrutinized this transaction and expended considerable energy and resources to arrange the entry of DISH as a fourth nationwide competitor, based on its successful history in other consumer industries and its vast holdings of spectrum, the most critical resource needed to compete in the RMWTS Markets. DISH's statements at trial persuade the Court that the new firm will take advantage of its

opportunity, aggressively competing in the RMWTS Markets to the benefit of price-conscious consumers and opening for consumer use a broad range of spectrum that had heretofore remained fallow.

- The Court remains fully mindful that among its various likely prospects, one possibility a merger of this magnitude raises is that of a less competitive future in the RMWTS Markets. However remote, that concern must be taken seriously. The Court, however, does not believe that such a possibility is reasonably likely in light of the numerous considerations discussed above. Accordingly, the Court concludes that Plaintiff States have failed to prove a violation of Section 7 and thus declines to enjoin the acquisition of Sprint by T-Mobile.

The DOJ issued a statement in which Assistant Attorney General Makan Delrahim argued "[t]his opinion is an important next step toward strengthening competition for high-quality 5G networks that will benefit American consumers nationwide." He added that "[a]s I have noted before, should a minority group of states, or even one, be able to undo the nationwide relief secured by the federal government, it would wreak havoc on parties' ability to merge, on the government's ability to settle cases, and cause real uncertainty in the market for procompetitive mergers and acquisitions."

New York Attorney General Letitia James explained in a statement that "[a]fter a thorough analysis, New York has decided not to move forward with an appeal in this case." She added that "[i]nstead, we hope to work with all the parties to ensure that consumers get the best pricing and service possible, that networks are built out throughout our state, and that good-paying jobs are created here in New York." James stated that "[w]e are gratified that this process has yielded commitments from T-Mobile to create jobs in Rochester and engage in robust national diversity initiatives that will connect our communities with good jobs and technology."

In contrast, California Attorney General Xavier Becerra's statement neither indicated whether the state would appeal or accept the decision. He asserted "our coalition is prepared to fight as long as necessary to protect innovation and competitive costs."

Moreover, it bears noting that the California Public Utility Commission still needs to adjudicate the deal, but a number of experts are claiming the state body cannot block a national deal the federal government has already approved. Nonetheless, the agency could not allow the merger to go ahead in California, the nation's largest market, which would likely lead to more litigation. The Commission has until July 12 to issue its decision, but this could happen much sooner.

In 2019, the DOJ and the FCC greenlit the merger. On November 8, the DOJ released its responses to comments on the proposed final judgment on the T-Mobile/Sprint merger. The DOJ claimed that

> the remedy the United States obtained addresses the competitive harm alleged in this action and is in the public interest. Accordingly, the United States recommends no modifications to the proposed Final Judgment. This remedy, now adopted by the Attorneys General of eight states who have joined this lawsuit and endorsed by two more through comments in this proceeding, promises to expand output in the mobile wireless market and be a boon for American consumers. The Federal Communications Commission has concluded that the proposed transaction, as modified by the FCC's own set of conditions, would be in the public interest. In reaching this conclusion, the FCC recognized the significant benefits that the proposed Final Judgment would yield. Commenters in this proceeding recognize these

> benefits as well—the United States received 32 comments regarding the settlement, the majority of which were supportive of the merger and/or the proposed Final Judgment.

The DOJ claimed that

> The proposed Final Judgment provides for a substantial divestiture which, when combined with the mobile wireless spectrum already owned by DISH Network Corp. ("DISH"), will enable DISH to enter the market as a new 5G mobile wireless services provider and a fourth nationwide facilities-based wireless carrier. T-Mobile and Sprint must divest to DISH Sprint's prepaid businesses, including more than 9 million Boost Mobile, Virgin Mobile, and Sprint-branded prepaid subscribers, and make available to DISH more than 400 employees currently running these businesses. The proposed settlement also provides for the divestiture of certain spectrum assets to DISH, and it requires T-Mobile and Sprint to make available to DISH at least 20,000 cell sites and hundreds of retail locations. T-Mobile must also provide DISH with robust access to the T-Mobile network for a period of seven years while DISH builds out its own 5G network.

DOJ claimed that

> The United States expects the proposed Final Judgment will provide substantial long-term benefits for American consumers by ensuring that large amounts of currently unused or underused spectrum are made available to American consumers in the form of advanced 5G networks that this proposed Final Judgment will help facilitate. Under commitments made to the FCC that have been incorporated into the proposed Final Judgment, DISH, which has been joined as a defendant in this action, is required to bring its existing spectrum resources online in a nationwide, greenfield 5G wireless network or risk substantial penalties at the FCC and in this Court. Under T-Mobile's commitments to the FCC, which are also incorporated into the proposed Final Judgment, the merged firm will combine T-Mobile's and Sprint's existing complementary spectrum resources and build out a 5G network to deliver network capacity that exceeds the sum of what either carrier could achieve on its own.

On November 5, a split FCC "issued a Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification approving—with conditions—the transfer of control applications filed by T-Mobile and Sprint" according to its press release. The vote was 3-2 to approve the proposed merger with conditions that would offset some of the anti-competitive effects of the U.S.'s third and fourth largest wireless providers.

The FCC contended that it "found that the transaction will help close the digital divide and advance United States leadership in 5G, the next generation of wireless connectivity." The Commission asserted that "[s]pecifically, T-Mobile and Sprint have committed within three years to deploy 5G service to cover 97% of the American people, and within six years to reach 99% of all Americans…[including] deploying 5G service to cover 85% of rural Americans within three years and 90% of rural Americans within six years." The FCC added that "[t]he parties also pledged that within six years, 90% of Americans would have access to mobile service with speeds of at least 100 Mbps and 99% of Americans would have access to speeds of at least 50 Mbps." The FCC added that "[t]his includes two-thirds of rural Americans having access to mobile service with speeds of at least 100 Mbps, and 90% of rural Americans having access to speeds of at least 50 Mbps."

The FCC stated that it

> conditioned its approval of the transaction on the parties fulfilling these commitments. Compliance with these commitments will be verified by rigorous drive-testing, overseen by an independent third party and subject to Commission oversight, to ensure that the service Americans receive will be what the parties have promised. And in order to ensure that these commitments are met, the parties will be required to make payments that could reach over two billion dollars if they do not meet their commitments within six years. Moreover, the parties will be required to make additional payments until they have fulfilled their commitments.

In the Memorandum Opinion, the FCC claimed

- As the two smallest nationwide mobile service providers, T-Mobile and Sprint assert that their combination will enable the deployment of a world-leading 5G network with capabilities beyond those either could achieve alone. Although each company had independent 5G plans, they claim that on their own they lack the capability to deploy 5G as broadly and with as much capacity as the resulting combined company, New T-Mobile, would. They maintain that their combined scale will increase network efficiency and that Sprint's mid-band spectrum will complement T-Mobile's low-band spectrum, further increasing the quality of their combined network. T-Mobile and Sprint also claim that these and other synergies will enable the merged firm to compete more effectively against the market leaders, AT&T and Verizon Wireless, than could either firm individually. As a result, they argue, the transaction would not result in the lessening of competition often associated with consolidation between horizontal competitors.
- Expanding 5G access to all Americans will also enhance the benefits of 5G innovation for the overall United States economy and will support American technological leadership. The larger the United States' 5G user base, and the broader its nationwide coverage, the greater the opportunity for entrepreneurs and innovators. The network benefits of the T-Mobile/Sprint transaction will thus extend beyond mobile wireless services alone, to enhance the competitiveness of the United States' economy.

The FCC further contended that

> At the end of the day, we believe that it is likely, even without conditions, that these competitive benefits will outweigh pricing pressure in certain areas, such as rural markets, and in certain segments of the market, such as consumers who are primarily quality-conscious. However, we are not confident that this will be the case across the board. In particular, based on the record, we are concerned about the impact of an unconditioned transaction on consumers in densely-populated areas who are primarily concerned about cost. Accordingly, we require, as a condition of our approval, that the Applicants fulfill a series of commitments to address the potential for lost price competition, such as the divestiture of Boost Mobile. These conditions eliminate the concerns otherwise identified in our review. Among other requirements, the Applicants have committed that the divested Boost Mobile will have low-cost wholesale network access on terms superior to typical MVNOs, with the financial incentive to provide robust competition from the moment of divestiture, and with the ability to build its own facilities over time. We conclude that, as

conditioned, the transaction would not substantially lessen competition,14and would be in the public interest.

In her dissenting statement, Commissioner Jessica Rosenworcel argued:

- The proposed tie-up of T-Mobile and Sprint will reduce competition. This merger will combine two of the four nationwide competitors in the wireless industry in the United States. As a result, three companies will control 99 percent of the wireless market. By any metric, this transaction will raise prices, lower quality, and slow innovation, just as we start to deploy the next-generation of wireless technology.
- We've all seen what happens when market concentration increases following a merger. A condensed airline industry brought us baggage fees and smaller seats, even as the price of fuel fell. A condensed pharmaceutical industry has led to a handful of drug companies raising the prices of lifesaving medications, taking advantage of those struggling with illness. There's no reason to think the mobile-phone industry will be different. Shrinking the number of national providers from four to three will hurt consumers, harm competition, and eliminate thousands of jobs. In deciding to overlook these harms, the Federal Communications Commission and the Department of Justice have been wooed by a few unenforceable concessions and hollow promises from the two companies involved.

Rosenworcel stated

- Moreover, the remedies the FCC and the Department of Justice design around these promises betray the free-market principles that for decades have made us the world's leader in wireless. Instead of promoting vigorous competition among providers, today's order justifies increased concentration by jerry-rigging a new provider dependent on the government dictating who sells what to whom and when. In addition, the agency retreats from nimbler and more decentralized approaches to spectrum management—like flexible use licenses and technology-neutral rules—that have served us so well in the past. To add insult to injury, it made these choices behind closed doors with a remarkable lack of transparency.
- Both the FCC and Department of Justice should know better than to think that tinkering around the edges of this deal can save it. Across our economy and across our geography, we are already struggling with the consequences of a seemingly never-ending wave of mergers and lax enforcement. So many of America's most pressing economic and political problems can be traced back to this kind of market consolidation. This includes dwindling opportunity in rural America as farmers struggle against agriculture conglomerates. It includes plunging rates of entrepreneurship as concentrated markets choke off small businesses. It includes falling wages as mergers reduce the need for employers to compete to keep their workers. And it includes income and wealth inequality that are higher than they've been in a hundred years.

In their complaint, the attorneys general of New York, California, Virginia, and other states claimed

> On April 29, 2018, T-Mobile and Sprint agreed to combine, a decision supported by their respective controlling shareholders, Deutsche Telekom AG, Deutsche Telekom Holding B.V., and Softbank Group Corp. The proposed transaction would eliminate Sprint as a competitor and reduce the number of MNOs with nationwide networks in the United States from four

> to three. The combined company would have a retail market share larger than the two largest MNOs today, Verizon and AT&T. In some areas, including in the New York City metropolitan area, the combined company's share of subscribers would exceed 50%. The combined market share of Sprint and T-Mobile would result in an increase in market concentration that significantly exceeds the thresholds at which mergers are presumed to violate the antitrust laws. This increased market concentration will result in diminished competition, higher prices, and reduced quality and innovation.

They further claimed

> The cumulative effect of this merger, therefore, will be to decrease competition in the retail mobile wireless telecommunications services market and increase prices that consumers pay for mobile wireless telecommunications services. Preliminary estimates based on the submissions made by economists for Sprint and T-Mobile show that the merger could cost Sprint and T-Mobile subscribers at least $4.5 billion annually and the harm to all retail mobile wireless telecommunications subscribers could be even larger. The merger will also negatively impact the entire ecosystem of businesses and significant segments of the American economy that depend on mobile wireless telecommunications services.

The attorneys general are asking that T-Mobile and Sprint "be permanently enjoined from and restrained from carrying out the Merger."

UK Lays Out Plan On "High-Risk Vendors" In 5G

An agency of the United Kingdom's (U.K.) government has released its recommendations and guidance on how the British telecommunications sector and government should address risk in building out its 5G networks. The U.S. government had been pressing the U.K. government, among other allies and nations, to not use Huawei's products to move into 5G because of alleged security risks that would allow the Chinese government to access communications. However, Prime Minister Boris Johnson's government declined to ban Huawei and instead has formulated an approach to manage risks emanating from "high-risk vendors." However, this approach builds on the U.K.'s existing treatment of risky vendors, most notably Huawei.

The National Cyber Security Centre (NCSC), which is housed within the Government Communications Headquarters (GCHQ), issued a summary of its security analysis of the U.K.'s telecommunications sector. This document "summarises the NCSC's technical recommendations for improving the security of the UK's telecoms sector, alongside a description of our technical security analysis that we used to derive these recommendations."

In a blog posting, NCSC Technical Director Dr. Ina Levy explained that "[d]ue to security and market sensitivities, it's not possible to publish the full analysis and response, but we do want to explain the work behind our cyber security advice to ministers." Levy explained "[i]f we determine a vendor to be high risk vendor, a number of things become necessary:

- Firstly, we ban them from being used in any of the sensitive functions that we need a network to have – things we've previously labelled as 'core', but it also includes other sensitive things like the legal intercept system and so on. We also continue to restrict their use in other critical infrastructure sectors, safety related and safety critical system and sensitive government, military and intelligence systems.

- Secondly, we put a cap on the amount of the access network a high risk vendor can provide equipment for. The cap balances two different security and resiliency risks; the first is the risk associated with high risk vendors and the second is the need for diversity of supply. The cap at 35% ensures the UK will not become nationally dependent on a high risk vendor while retaining competition in the market and allowing operators to continue to use two Radio Access Network (RAN) vendors. The calculation of 35% is also interesting. We've been quite subtle about how we calculate that – it's important to make sure it can't be easily gamed, for example by using an HRV's basestations in all the cities and a non-HRV's products in the countryside.
- That starts to constrain any high risk vendor, but we also need to put in place a bespoke mitigation strategy for each high risk vendor. That requires things that only an agency like NCSC can do. For Huawei, this will be an evolution of the existing mitigation strategy, including but not limited to HCSEC ('the cell') which does things for us.
- Finally, we also need to make sure that those operators who choose to use high risk vendors like Huawei understand the risks properly and design their networks, support and operational systems and processes to manage those risks. That means we'll have to help them. NCSC has a mandate from government as the UK's national technical authority for cyber security, responsibility for the long-standing Huawei mitigation strategy, knowledge of other vendor practices, access to national intelligence machinery, a world class vulnerability research team, international partnerships and the data, skills and capabilities to inform how the risks can be sensibly managed.

Levy stated that

- GCHQ has been dealing with Huawei in the UK telecoms sector since 2003, first through CESG and now through the NCSC. We've always treated them as a 'high risk vendor' and have worked to limit their use in the UK and put extra mitigations around their equipment and services. We've never 'trusted' Huawei and the artefacts you can see (like the Huawei Cyber Security Evaluation Centre (HCSEC) and the oversight board reports) exist because we treat them differently to other vendors.
- We ask operators to use Huawei in a limited way so we can collectively manage the risk and NCSC put in place a wider mitigation strategy, of which HCSEC is the most visible part. Even before HCSEC was set up in 2010, we were doing similar work but through a different mechanism. Technology has obviously evolved since that time and our security mitigation strategy, both generally and vendor specific, has had to evolve with it. The move to 5G is another evolution of the technology and our security mitigations need to evolve again.

In the summary of the security analysis, NCSC stated that

> As technologies grow and evolve, we must have a security framework that is fit for purpose and ensures the UK's Critical National Telecoms Infrastructure remains online and secure both now and in the future. The findings of the Department for Digital, Culture, Media and Sport (DCMS) Supply Chain Review show that there is much work to be done. The review recommended the establishment of a new, robust security framework for the UK telecoms sector, with a set of new Telecoms Security Requirements (TSRs) at its heart. These TSRs will provide clarity to telecoms operators. Their implementation will ensure that operators operate secure and resilient networks and manage their supply chains appropriately.

NCSC made recommendations that "fall into five categories:

- TSRs detailing how operators should reduce their most significant cyber risks
- advice to government and industry on the management of High Risk Vendors (HRVs)
- diversification of the infrastructure market
- the establishment of a National Telecoms Lab to perform a broad range of testing of the UK's telecoms networks and equipment
- continued regular and detailed threat-driven security testing of operators' networks, as performed under Ofcom's TBEST scheme

NCSC has long been grappling with the security issues posed by Huawei. During his February 2019 CyberSec speech in Brussels, NCSC CEO Ciaran Martin spoke on the rollout of 5G and continued cooperation with European partners aside and apart from Brexit. Regarding Huawei, Martin stated that "Huawei's presence is subject to detailed, formal oversight, led by the NCSC." He said that "[b]ecause of our 15 years of dealings with the company and ten years of a formally agreed mitigation strategy which involves detailed provision of information, we have a wealth of understanding of the company." Martin explained that "[w]e also have strict controls for how Huawei is deployed…[i]t is not in any sensitive networks – including those of the government…[and] [i]ts kit is part of a balanced supply chain with other suppliers."

In 2019, Huawei responded to a British Parliament committee and explained that it would spend $2 billion over five years in large part to remediate the shortcomings turned up by a British government oversight board. Huawei stated that this funding will "help ensure that our products are better prepared for a more complex security environment both now and in the future." In January, the Chair of the House of Commons Science and Technology Committee wrote Huawei with his concerns about the United Kingdom's communications infrastructure in light of three Five Eyes nations' actions to reduce the roles of Chinese firms in their systems and China's recently enacted National Intelligence Law. In its annual report in July 2018, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board found that "[d]ue to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated."

In April, HCSEC released its fifth annual report and found that Huawei has failed to address the issues turned up in the 2018 report. Notably, in its 2018 report, the Board stated "[d]ue to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated." In this year's report, the Board stated that "[n]o material progress has been made on the issues raised in the previous 2018 report."

The Board stated that its work "has continued to identify concerning issues in Huawei's approach to software development bringing significantly increased risk to UK operators, which requires ongoing management and mitigation." The Board asserted that it "continues to be able to provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK" and "advises that it will be difficult to appropriately risk-manage future products in the context of UK deployments, until the underlying defects in Huawei's software engineering and cyber security processes are remediated." The Board stated that it "has not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation programme that it has proposed as a means of addressing these underlying

defects." The Board explained that it "will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC…[and] can only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term."

Further Reading

- "Senior intelligence official told lawmakers that Russia wants to see Trump reelected" – *Washington Post* and "Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump" – *New York Times*. According to these accounts of a briefing provided to the House Intelligence Committee by the Office of the Director of National Intelligence (DNI), the status report on ongoing, mutating Russian efforts to interfere with the 2020 election may both result in the acting DNI being denied the job permanently and an impairment of federal efforts to fend off Russian interference. Reportedly, the conclusion that Russia favors Trump over Democratic candidates angered both committee Republicans and the White House. With the departure of former acting DNI Joseph Maguire and the tapping of U.S. Ambassador to Germany Richard Grenell, a Trump loyalist with no intelligence experience, the Intelligence Community (IC) may limit the information it shares with Congress and the public.
- "Pay Up, Or We'll Make Google Ban Your Ads" — *Krebs on Security*. A variation of ransomware has surfaced in which the purveyors threaten to overwhelm a website's advertising through Google's AdSense with bot traffic, causing Google to take down the ad, unless bitcoin is turned over. Another mutation of the seemingly lucrative ransomware trade.
- "2014 Bloomberg Hoped the NSA Was "'Reading Every Email'" – *The Intercept*. The website unearthed a live event with Katie Couric at which former New York City Mayor and candidate for the Democratic nomination for President Mike Bloomberg endorsed National Security Agency surveillance and a notice and comment approach to privacy regarding private sector practices. However, these views are contrary to many in the Democratic party, and Bloomberg has taken other privacy and surveillance stances that may prove unacceptable to Democratic voters.
- "Retail Customer Data Exposure Spotlights Cloud Security Risk" – *Bloomberg Law*. Failing to properly set up the security for consumer data stored in the cloud resulted in a security firm being able to easily access information on millions of American households. A market analytics company did not configure security settings correctly and consequently the data on consumers being stored on Amazon's cloud was accessible to anyone with credentials to log into AWS.
- "Hacker Eva Galperin Has a Plan to Eradicate Stalkerware" – *WIRED*. A security researcher with the Electronic Frontier Foundation (EFF) has convinced Kaspersky to treat spyware used by stalkers and estranged spouses as malware and hopes to talk the other antivirus companies into doing the same.
- "At Facebook, One Million Takedowns Per Day is Evidence of Failure, Not Success" – *Council on Foreign Relations*. In this piece, a cybersecurity expert argues that even if Facebook's numbers on takedowns of fake accounts are accurate, there are still millions of fake accounts from which users may sow discord and disinformation. A case is made for Facebook to introduce validated accounts to ensure the person opening the account is an actual person and not a mischief maker.

- "Corporations are working with the Trump administration to control online speech" – *Washington Post*. In an opinion piece, Senator Ron Wyden (D-OR) defended Section 230 the same week the Department of Justice held a workshop on this provision of federal law that protects online platforms from legal liability for what its users post online. Following months of Trump Administration and Republican pushback on Section 230, Attorney General William Barr called for a reexamination of the legal shield. Wyden claimed the Administration and Republicans are looking to revise Section 230 with the foreseeable results that smaller platforms and those expressing disfavored viewpoints would be either litigated out of existence or silenced.
- "Lawyer: Assange was offered US pardon if he cleared Russia" – *AP News* and "Rohrabacher confirms he offered Trump pardon to Assange for proof Russia didn't hack DNC email" – *Yahoo News*. Despite differing rationales as to why a U.S. pardon was being offered, both an attorney for Julian Assange and former Representative Dana Rohrabacher (R-CA) agree that a pardon was offered to Assange if he disclosed the source of the Democratic National Committee emails provided to Wikileaks. Assange's lawyer claimed the pardon would be in exchange for stating Russia was not involved whereas Rohrabacher claimed the purpose was to confirm that deceased DNC staffer Seth Rich was the source. The White House denied any involvement.
- "How Saudi Arabia Infiltrated Twitter" – *BuzzFeed News*. This piece details the lack of internal security at Twitter that made the social media platform ripe to be infiltrated. Allegedly, two Saudis working for Twitter were recruited to inform the Saudi government about the Twitter accounts of Saudi dissidents throughout the world. One employee has been indicted and is being held in the U.S. while the other fled to Saudi Arabia. Moreover, the article suggests the U.S. and Israeli governments tried to get Twitter to turn over account information, but the company declined to do so.