Cyber Update
10 April 2019
By Michael Kans, Esq.

Bill To Restore Net Neutrality Moves Out of Committee

On April 3, the House Energy and Commerce Committee marked up and reported out the "Save the Internet Act of 2019" (H.R. 1644) that would undo the Federal Communications Commission's (FCC) repeal of the Obama Administration's 2015 net neutrality order and reclassify internet service providers (ISPs) under Title II of the Federal Communications Act as common carriers. The bill would also negate the FCC's more recent order, FCC 17–166, aka "Restoring Internet Freedom," that returned ISPs to their previous regulatory posture as being regulated under Title I as information services and bar the FCC from classifying ISPs this way. The bill would reimplement FCC 15–24, aka the Open Internet Order, and the accompanying regulations except that ISPs with fewer than 100,000 subscribers would be exempted from the transparency rule's "performance characteristics and network practices" for one year.

The 2015 regulations put in place "bright-line rules that prohibit blocking, throttling, and paid prioritization; a rule preventing broadband providers from unreasonably interfering or disadvantaging consumers or edge providers from reaching one another on the Internet; and provides for enhanced transparency into network management practices, network performance, and commercial terms of broadband Internet access service." However, the FCC's 2017 rollback of net neutrality regulations "restore[d] the classification of broadband internet access service as a lightly-regulated information service and reinstates the private mobile service classification of mobile broadband internet access service….requires ISPs to disclose information about their network management practices, performance characteristics, and commercial terms of service…[and] eliminates the conduct rules imposed by the [2015 regulations]."

In their memorandum for the subcommittee markup of H.R. 1644, Democrats claimed

> The repeal of the 2015 Order has had broad implications for consumers and small businesses accessing the internet. Under the 2015 Order, the FCC was obligated to enforce explicit prohibitions on blocking, throttling, and pay-for-priority arrangements. The FCC also retained its authority to address future discriminatory, unreasonable, or unjust network practices. The repeal removed protections for people with disabilities that previously ensured their access to broadband service. The repeal also did away with provisions that ensured fair access to utility poles, ducts, conduits, and rights-of-way. Finally, by relinquishing the FCC's authority to accelerate deployment of broadband, the repeal undermined the FCC's authority to fund rural broadband access and adoption efforts for low-income individuals.

In their dissenting views in the Committee Report, Republicans stated

> The internet grew to become the single most important driver of economic growth, job creation, and a better quality of life for all Americans before the FCC imposed heavy-handed Title II regulations on ISPs in 2015. The FCC's 2015 Order, under the direction of President Obama, was a sharp but brief detour from years of bipartisan consensus that the internet should be regulated as an "information service" under Title I. In the two years of

> the Obama FCC's Title regulations, broadband network investment declined by over $3 billion—or more than 5 percent. This was the first such decline outside of a recession in the internet era and was due, in large part, to the uncertainty Title II imposed on ISPs. In addition to impairing investment, Title II hindered innovation under the FCC's amorphous general conduct standard.

Big picture, this bill is mostly about messaging and articulating Democratic priorities on technology issues while putting Republicans on the opposite side of what Democrats consider a winning political issue. H.R. 1644 has 197 sponsors, is likely to go to the House floor, and is also likely not to pass the Senate. In the last Congress, the Senate passed a resolution (S.J.Res.52) to undo the FCC's regulations to restore the status quo ante net neutrality, but the Republican-controlled House did not act on the legislation that would have used the Congressional Review Act to negate the FCC's regulations even though there were 171 cosponsors for identical legislation introduced in the House. While the Senate vote tally on S.J.Res.52 (52-47) suggests H.R. 1644 could possibly pass the Senate, and even if Senate Majority Leader Mitch McConnell (R-KY) were to allow the bill a majority vote (as opposed to a 60 vote threshold necessary to end a filibuster or under an unanimous consent agreement), the Trump Administration has already threatened to veto the bill.

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 this court is hearing a challenge to the FCC's 2017 order in *Mozilla v. FCC*.

5G Reports and Legislation

Last week, an advisory body to the Pentagon drafted a report on the options facing the Department of Defense (DOD) as the U.S. and other nations are on the cusp of transitioning to the next generation of wireless networks that promise even faster speeds that will likely drive the development of new applications and devices. The Defense Innovation Board (Board) released "THE 5G ECOSYSTEM: RISKS & OPPORTUNITIES FOR DOD" to "insight into the commercial landscape as well as the DOD landscape to give a comprehensive view of the stakeholders and future of 5G." The Board explained that "[t]he shift from 4G to 5G will drastically impact the future of global communication networks and fundamentally change the environment in which DOD operates." The Board conceded that "[w]hile DOD will feel the impact of 5G, the rollout itself will be driven by the U.S. commercial sector."

The Board explained

> The term "5G" refers to the oncoming fifth generation of wireless networks and technology that will produce a step-change improvement in data speed, volume, and latency (delay in

> data transfer) over fourth generation (4G and 4G LTE) networks. 5G will enable a host of new technologies that will change the standard of public and private sector operations, from autonomous vehicles to smart cities, virtual reality, and battle networks. Historical shifts between wireless generations suggest that the first-mover country stands to gain billions in revenue accompanied by substantial job creation and leadership in technology innovation. First movers also set standards and practices that were then adopted by subsequent entrants. Conversely, countries that fell behind in previous wireless generation shifts were obligated to adopt the standards, technologies, and architectures of the leading country and missed out on a generation of wireless capabilities and market potential.

The development of 5G will require the bonding together of 100 MHz channels to deliver faster speeds in new spectrums. The Board explained that the U.S., Japan, and South Korea are looking at using the electromagnetic spectrum frequencies between 24 and 300 GHz (aka mmWave) for 5G while other nations, like China, are looking at using the 3 and 4 GHZ range (aka sub-6) for 5G networks. Moreover, in the U.S., the DOD uses the latter spectrum, meaning that any transition could be tricky for 5G using that band of spectrum. The Board noted that "U.S. carriers are primarily focused on mmWave deployment for 5G because most of the 3 and 4 GHz spectrum being used by the rest of the world for 5G are exclusive Federal bands in the United States, extensively used by DOD in particular."

The Board added that

> Spectrum bands in the 3 and 4 Ghz range dominate global 5G activity because of improved propagation (range) over mmWave spectrum, resulting in far fewer base stations needed to be deployed to deliver the same coverage and performance. Because large swaths of the sub-6 bands in the United States are not available for civil/commercial use, U.S. carriers and the FCC (which controls civil spectrum in the US) are betting on mmWave spectrum as the core domestic 5G approach.

The Board stated that "[b]oth DOD and the FCC are currently prioritizing mmWave over sub-6 mid-band spectrum with a particular focus on the 28 and 37 GHz bands, but this is a fundamentally flawed focus due to the impracticality of mmWave deployment." The Board stated that "DOD must prepare to operate in a sub-6 5G ecosystem, which will require a shift in strategy and a consideration of where DOD is willing to share bandwidth in the sub-6 realm."

The Board explained that

> However, 5G also presents a serious potential risk for DOD going forward. When operating overseas in the future, the vast majority of these networks and systems may depend on 5G infrastructure. If China leads the field in 5G infrastructure and systems, then the future 5G ecosystem will likely have Chinese components embedded throughout. This would pose a serious threat to the security of DOD operations and networks going forward. Additionally, the growth in the number of connected devices increases the potential "attack surface" for adversaries to target across DOD networks, which will require increased vigilance and security across systems. The larger volume of data being transferred will complicate this task, as it will make it more difficult to detect malicious traffic on a network.

The Board asserted that "5G has the ability to enhance DOD decision-making and strategic capabilities from the enterprise network to the tactical edge of the battlefield…[and] will increase DOD's ability to link multiple systems into a broader network while sharing information in real time, improving communication across Services, geographies, and domains while developing a common picture of the battlefield to improve situational awareness." The Board claimed that "[t]his improved connectivity may in turn enable a host of new technologies and missions, from hypersonics and hypersonic defense to resilient satellite constellations and mesh networks."

The Board made the following recommendations:

- DOD needs to make a plan for sharing sub-6 GHz spectrum to shape the future 5G ecosystem, including an assessment of how much and which bandwidths need to be shared, within what timeframe, and how that sharing will impact DOD systems.
- DOD must prepare to operate in a "post-Western" wireless ecosystem. This plan should include R&D investments towards system security and resiliency on an engineering and strategic level.
- DOD should advocate for adjusted trade policies to discourage vulnerabilities in its supply chain on the grounds that they put national security assets and missions at risk.

In response to some of the threats posed by Huawei and other Chinese firms regarding the 5G rollout, a Senate Committee reported out a bill, and another was introduced in the House. The Senate Commerce, Science, and Transportation Committee marked up and reported out the "Eliminate From Regulators Opportunities to Nationalize The Internet In Every Respect Act" (E-FRONTIER Act) (S. 918) that would bar the executive branch from "construct[ing], operat[ing], or offer[ing] wholesale or retail service on a broadband network unless a duly enacted of Congress signed into law by the President provides the President or the agency, as applicable, with that authority." The Government Accountability Office (GAO) would be required to report on and analyze foreign threats to U.S. broadband providers and networks and recommendations on reducing any such vulnerabilities. A companion bill has been introduced in the House (H.R. 2063) that has not yet been acted upon. These bills were introduced in response to media reports that the Trump Administration had prepared a memorandum that posed the nationalization of the still-to-be-built 5G networks as a possible policy option.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) released a report titled "Huawei, 5G and China as a Security Threat" that "examines the cybersecurity debate around Huawei as the potential supplier of 5G technology for next generation wireless networks."

CCDCOE stated

> The authors argue that the issue of Huawei 5G deployment must be assessed in the broader geopolitical context. First, China approaches it as such. Its legal and political environment, along with its known practice of 'public-private partnership' in cyber espionage, remain a concern. Secondly, the role of fundamental digital infrastructure for modern societies is not a mere technocratic platform issue. Neither can the 5G discussion be isolated to the civilian or the defence domain. It has critical implications for both simultaneously, and choices must therefore be informed by both perspectives.

CCDCOE offered the following recommendations:

- **5G rollout needs to be recognised as a strategic rather than merely a technological choice.** Solutions chosen today will steer and limit the choices available for years to come. Given the complexity of socioeconomic and security issues affected by the decision to

deploy backbone digital infrastructure, the issue of welcoming or refusing Huawei or other Chinese providers cannot be left for technocrats alone to resolve. It requires the political will to step out of the comfort zone and tackle complex aspects of technology, economy and security, the effect of which will span well beyond parliamentary election terms.

- **A shared concern necessitates a coordinated response.** The dilemma at hand primarily concerns civilian networks, so it is not overly likely that NATO will take a lead in coordinating action. However, the NATO Alliance is, and will remain, an important venue for allies and partners for sharing information on threats, and that capacity should not be viewed as separate from defining a common approach among liberal (and European in particular) democracies. The issue of Huawei technology is, however, not without relevance to the Alliance. NATO depends of national critical infrastructure to execute national operations and missions. Infrastructure security issues may affect NATO networks or deployed networks such as the Federated Mission Network. Such networks can also be exposed to risk because their extensions may use host nation civilian infrastructure.
- **One size does not fit all: there is a need for nuanced risk awareness and risk management tools.** Certainly, there are no easy responses to this dilemma. Shutting the door to cooperation with Huawei and China may backfire, as it deprives European and other regional industries of a chance to develop 5G services. This leaves development to be driven by Chinese companies, which can well afford it given the scope and growing purchasing power of their home market and their active engagement with developing countries as growing future markets for new technology.
- **Finally, risks associated with investments and takeovers by foreign capital are structural and are not specific to digital infrastructure.** With a binary choice of 'take it or leave it' not among the options – there are as of yet no equivalent alternatives to Huawei 5G technology; the West is neither able nor willing to afford a technological stagnation, and with the expected socioeconomic benefits in the promise of 5G, states will likely remain pragmatic in their approaches. Whether by issuing security guidance to reinforce the security of critical government and commercial functions, strengthening risk assessment and management processes, or agreeing on transparency and accountability mechanisms, national responses will likely seek to improve risk mitigation.

White House Memo on Counterfeit Goods

Last week, President Donald Trump signed a memorandum "to protect American businesses, intellectual property rights holders, consumers, national and economic security, and the American public from the dangers and negative effects of counterfeit and pirated goods, including those that are imported through online third-party marketplaces and other third-party intermediaries." This directive orders the Department of Homeland Security and other agencies to craft a report on how third-party marketplaces and third-party intermediaries are used by counterfeiters to sell fake and knock off goods to U.S. consumers, including recommendations on "appropriate administrative, statutory, regulatory, or other changes, including enhanced enforcement actions, that could substantially reduce trafficking in counterfeit and pirated goods or promote more effective law enforcement regarding trafficking in such goods."

This memorandum may intentionally or not strike at two of Trump's favorite targets: China and Amazon. China stands accused of being the world's foremost counterfeiter of goods and pirate of intellectual property, while the owner of Amazon, Jeff Bezos, and the newspaper he owns, the *Washington Post*, have often been at odds with a number of the Administration's policies. *The Verge* compiled the back and forth between Trump and Amazon.

In the press rollout, the Administration made quite clear that memorandum pertains to companies like Amazon, Alibaba, e-Bay and others, and Assistant to the President and Director of the Office of Trade and Manufacturing Policy Peter Navarro said "[t]his is a warning shot across the bow that it is your job to police these matters, and if you won't clean it up the government will." However, Navarro dismissed questions about whether the memorandum was designed to pressure China and Amazon.

The memorandum also requires investigation into the Department of Defense's efforts to secure its supply chain. The DHS report "should also evaluate the effectiveness of Federal efforts, including the requirement for certain Federal contractors to establish and maintain a system to detect and avoid counterfeit electronic parts under the Defense Federal Acquisition Regulation Supplement (DFARS) 252.246-7007, as well as steps taken by foreign governments, such as France and Canada, to combat trafficking in counterfeit and pirated goods." This could potentially affect how the Office of Management and Budget (OMB) and General Services Administration (GSA) establish e-Commerce portals required under Section 846 of the FY 2018 National Defense Authorization Act (NDAA), for the Administration has made clear they consider third-party counterfeits a national security problem given the Pentagon's supply chain. The e-Commerce initiative may need to address counterfeits and piracy in response to the report DHS will deliver.

Within seven months, DHS, in conjunction with other stakeholder agencies, must submit a report that includes the following among other elements:

- Analyze available data and other information to develop a deeper understanding of the extent to which online third-party marketplaces and other third party intermediaries are used to facilitate the importation and sale of counterfeit and pirated goods; identify the factors that contribute to trafficking in counterfeit and pirated goods; and describe any market incentives and distortions that may contribute to third-party intermediaries facilitating trafficking in counterfeit and pirated goods.
- Evaluate the existing policies and procedures of third-party intermediaries relating to trafficking in counterfeit and pirated goods, and identify the practices of those entities that have been most effective in curbing the importation and sale of counterfeit and pirated goods, including those conveyed through online third-party marketplaces.
- Identify appropriate administrative, statutory, regulatory, or other changes, including enhanced enforcement actions, that could substantially reduce trafficking in counterfeit and pirated goods or promote more effective law enforcement regarding trafficking in such goods. The report should address the practices of counterfeiters and pirates, including their shipping, fulfillment, and payment logistics, and assess means of mitigating the factors that facilitate trafficking in counterfeit and pirated goods.
- Identify appropriate administrative, regulatory, legislative, or policy changes that would enable agencies, as appropriate, to more effectively share information regarding counterfeit and pirated goods, including suspected counterfeit and pirated goods, with intellectual property rights holders, consumers, and third-party intermediaries.

DHS' Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) enforce U.S. laws against intellectual property rights violations at U.S. borders, while other agencies play roles in the issue of counterfeiting and pirating more broadly. In a report last year, the Government Accountability Office (GAO) explained the lines of authority the two agencies have:

> CBP's responsibilities include identifying and seizing IPR-infringing goods at the U.S. border, a function that also includes assessing penalties and denying entry to certain types of IPR-infringing goods. ICE's responsibilities include investigating IPR violations, building cases for federal prosecution, and serving as the lead agency for the IPR Center. CBP employs a risk-based approach that uses targeting and other tools to identify for further examination a selection of imported goods that have arrived at U.S. ports; when violations are found, CBP seizes infringing goods and may refer cases to ICE for criminal investigation.

The GAO found "20 of 47 items GAO purchased from third-party sellers on popular consumer websites were counterfeit, according to testing by the products' rights holders…highlighting potential risks to consumers."

The GAO noted that

> Counterfeit goods provide a lucrative market for criminal activity and can pose serious risks to consumers. Growth in e-commerce has changed the way counterfeiters interact with consumers, and the accompanying increase in the volume and sophistication of counterfeit goods has created challenges for CBP and ICE enforcement. While CBP and ICE have undertaken activities to enhance IPR enforcement and collected some performance data on their activities, CBP has conducted limited evaluation of its efforts. Managing the huge volume of both legitimate and counterfeit goods entering the country requires efficient use of resources. Without better information on the effectiveness of its activities, CBP may not be able to focus its resources on the most efficient or effective efforts. Additionally, without collecting and disseminating effective practices resulting from port-led initiatives, CBP may be missing an opportunity to scale up or improve on existing efforts.

OPM Loosens Hiring For IT Professionals To Help CIOs

The Office of Personnel Management (OPM) has released a final rule pursuant to the May 2018 Executive Order (EO) 13833, "Enhancing the Effectiveness of Agency Chief Information Officers," that required OPM to issue "regulations delegating to the head of a covered agency authority necessary to determine whether there is a severe shortage of candidates or a critical hiring need for information technology (IT) positions, under criteria established by OPM." Section 9 of the EO "directed OPM to propose regulations pursuant to which OPM could delegate to the heads of certain agencies (other than the Secretary of Defense) authority to determine, under regulations prescribed by OPM, whether a severe shortage of candidates (or, for the U.S. Department of Veterans Affairs (VA) a severe shortage of highly-qualified candidates) or a critical hiring need exists for positions in the Information Technology Management series, general schedule (GS)-2210, for purposes of demonstrating a need for a Direct Hire Authority." This new rule puts in place that flexibility in hiring IT professionals for agencies and takes effect May 3, 2019.

However, it is an open question whether the balance of EO 13833, which was intended to implement long recommended and enacted CIO authorities, has been put in place by agencies as directed by the President. EO 13833 also directed the heads of all agencies (except the DOD) to take a number of steps, including:

- Ensuring that "the CIO of the covered agency reports directly to the agency head, such that the CIO has direct access to the agency head regarding all programs that include IT"
- Making the CIO "the primary strategic advisor to the agency head concerning the use of IT"

- Ensuring "the CIO has a significant role, including, as appropriate, as lead advisor, in all annual and multi-year planning, programming, budgeting, and execution decisions, as well as in all management, governance, and oversight processes related to IT; and
- the CIO of the covered agency approves the appointment of any component CIO in that agency."

Yet, public indications are that agencies have not taken these steps to meet their obligations under federal law, mainly FITARA, to empower CIOs. In December 2018, at a House Oversight and Government Reform Committee hearing on the FITARA scorecard, the GAO explained

> [I]n August 2018, GAO reported that none of the 24 selected agencies had policies that fully addressed the role of their CIO, as called for by laws and guidance. GAO recommended that OMB and each of the 24 agencies take actions to improve the effectiveness of CIOs' implementation of their responsibilities. As of November 2018, none of the 27 recommendations had been implemented.

These findings were echoed in the GAO's high risk list in February 2019.

It is not clear what follow up steps the Administration, likely through the Office of Management and Budget (OMB), or Congress may take in response to the continued failure of federal agencies to meet the statutory and regulatory requirements with respect to CIO authority.

Other Hearings and Events

"Mapping the Challenges and Progress of the Office of Information and Technology" – House Veterans Affairs/Technology Modernization
"MISSION Critical: Assessing the Technology to Support Community Care" – House Veterans Affairs

Further Reading

"Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned" – *ProPublica*
"Millions of Facebook Records Found on Amazon Cloud Servers" – *Bloomberg*
"YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant" – *Bloomberg*
"Hunting for clues in hacking's cold cases" – *E&E News*
"Current, former Pentagon leaders sound alarm on Chinese technology in 5G networks" – *Washington Post*
"Ancestry-Testing Company: It's Our 'Moral Responsibility' to Give The FBI Access to Your DNA" – *Gizmodo*