Statement before the Federal Communications Commission On Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership

IB Docket No. 16-155
DA 20-452
FRS 16720

ROSLYN LAYTON, PHD
Visiting Scholar

June 18, 2020

Thank you for the opportunity to comment on a Rule for the Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership.[1] Executive Order 1391 formalizes how the Executive Branch agencies (collectively "Team Telecom") and the Federal Communications Commission (FCC) work together. This is an essential reform to improve cyber defenses that have lagged for years and to streamline administrative processes. The order empowers the agencies to address directly long-neglected threats of the presence of telecommunications goods and services provided by adversarial foreign owners.[2]

The US faces an existential threat to its security from the Chinese government. This has been excessively documented but has been met with relatively limited policy response until recently. Sources for this information include some twenty years of reports from Congress' bipartisan United States China Commission, multiple reports from Defense and Intelligence agencies (in the US and allied countries), and investigations, reports, and cases from the Departments of Justice, Homeland Security, Commerce, Federal Bureau of Investigation, and countless security experts. In summary, the FCC should work with the Executive Branch agencies to restrict *broadly* Chinese-government owned equipment vendors from US communications networks. Huawei and ZTE are the tip of the iceberg of hundreds of Chinese government-owned and affiliated firms (with at least 10 percent government ownership) that supply products and services in US communications networks and which present significant security and privacy risks. Their applications to the FCC should be scrutinized, rejected, and revoked. For applications in which the FCC cannot determine the level of Chinese government ownership, they should be referred to Executive Branch agencies.

The FCC's current effort is needed and welcome. The FCC recognized in 2016 that there were significant process issues related to review of applications, and hence it adopted the Notice of Proposed Rulemaking to address them.[3] That the FCC revisits the Order now should be commended.

Importantly, the FCC takes pains to make its process clear, transparent, and explicit. For example, it gives applicants a clear path and timeline to engage with the FCC in answering inquiries. Moreover, FCC decisions can be challenged in court. American equipment providers are not afforded the same courtesies and due process in China.

This comment makes the following points:

[1] https://www.federalregister.gov/documents/2020/05/19/2020-09873/process-reform-for-executive-branch-review-of-certain-fcc-applications-and-petitions-involving

[2] https://www.aei.org/technology-and-innovation/the-team-telecom-executive-order-the-department-of-justice-and-china-telecom/

[3] https://www.fcc.gov/document/reforming-executive-branch-review-process

Security issues with firms whose owners are adversarial governments

Importantly, the Rule and Order focuses on applications from firms with 10 percent or more foreign ownership. Notably foreign owners are not inherently problematic. Indeed, the US benefits tremendously from foreign investment in US assets, on the order of hundreds of billions of dollars annually. The Bureau of Economic Analysis reports that more than two-thirds of the total foreign investment in the US comes from European investors; perhaps less than 5 percent of foreign investment comes from investors from adversarial states. However, it is important to scrutinize this ownership in the products and services that comprise communications networks, one of America's critical infrastructures.

Moreover, just because a company is owned by a foreign government in whole or part does not mean it presents a national security risk to the US. Indeed, many communications companies around the world have some government ownership. The issue for the US is whether the government in question presents a threat.

In the management of a firm, it is understood that owners, directors, officers, board members, and shareholders exercise control and influence in its decisions. A national government is the ultimate authority for a country; it creates and implements laws and maintains a military. A national government exerts control over the firm in the laws and requirements it imposes. A government that is the owner, director, shareholder, or controller of a firm has even greater leverage. As such, there is an issue when the applicant to the FCC is a firm with ownership by the Chinese government.

From the perspective of US security, there is an issue when a firm whose owners and government are one in the same, or are fungible, as is the case of China. In the US, a private firm has a buffer from the state and Constitutionally mandated rights of due process enforceable by an independent court system. China's institutions are not analogous to the US, nor do they behave in the same way nor have the same purpose. Unlike the US, China's military is not under civilian control, a prerequisite of a liberal democracy,[4] whereas the Chinese government is a fusion of the administrative state and the People's Liberation Army into a single entity.[5] China can direct its firms in a way that the US cannot, and China uses its ownership in firms to advance its interests.

In 2015 the Chinese government announced its "Made In China 2025" initiative, a plan for China to conquer the US as the world's technological leader and to dominate the core technologies of the future, including telecommunications. This is underpinned by China's larger "techno-nationalist" strategy of projecting global power through its corporate tech champions and accumulating hard currency through the sale of consumer goods and electronics to support its military projects around the globe and in space. The technology that China can't develop itself, it will acquire—with a preference for leading brands. The technology that China can't acquire, it will steal. China's documented strategy of "unrestricted warfare" includes significant information operations toward the US: the theft and hacking of intellectual property; surveillance and espionage of sensitive and strategic information activities; the collection and processing Americans' personal information; and the set of illegal practices like forced technology transfers, predatory pricing, strong-arm sales tactics, bribery, fraud, and corruption.

For example, foreign firms operating in China are forced to transfer their technology to Chinese

[4] https://www.amazon.com/Soldier-State-Politics-Civil-Military-Relations/dp/0674817362
[5] https://www.jstor.org/stable/655470

government-designated actors, are made to enter into joint ventures with Chinese firms, and may be required to surrender their source codes and other proprietary information. Firms are given quotas to limit the number of devices they can sell or caps on the market share they can serve. In many instances, they are blocked outright with no notice, explanation, or recourse

The National People's Congress of the Republic of China recently adopted Cybersecurity and Intelligence laws regulating how Chinese firms treat data on Chinese information technology, rules that apply to any Chinese-made technology anywhere, assert sovereignty over cyberspace, and authority over all data. Though there is debate as to how strictly these laws are interpreted and implemented, it is not inconceivable that the Chinese government could compel a Chinese firm to collect and transfer an American's user data to China for illicit processing. While European data protection laws prohibit such cross-border transfers, American lawmakers have been reluctant to fragment cyberspace further. On the other hand, the firm could keep the data in the US and still perform the Chinese government's desired processing, perhaps in an anonymized form. Because such illicit processing is indetectable from regular network operations, it nearly impossible to mitigate the risk by using a Chinese-government owned firm's product or service. Emmanuel Pernot-Leplay, PhD in comparative data protection law from Shanghai Jiao Tong University observes, "Governments worry less about what Chinese law says than what China's government can actually do."[6] For that reason, NATO, the US military, and the US federal government restrict their use of IT products and services from Chinese state-owned and affiliated entities.

Chinese companies are not necessarily transparent about their ownership, and this makes the FCC's job more difficulty, but also more important in its scrutiny. For example, Huawei is a company which claims to be private, but this is not independently certifiable. A comprehensive bipartisan report on Huawei was issued in 2012 by the US House of Representatives Permanent Select Committee on Intelligence.[7] The investigation included a visit to the company's Shenzhen headquarters and extensive interview with Huawei's leadership. Huawei could not provide complete information on its corporate structure and decision-making process; it admitted to having a Chinese Communist Party Committee within the company but would not disclose the members' identity; it could not provide evidence that it is independent of the Chinese government nor that its US operations were independent of its Chinese headquarters, undermining its claims that it's an independent subsidiary. Huawei could not answer questions about historical ties to the Chinese military, preferential treatment by the government for tax fraud abuse, or its relationship to foreign consulting firms. Such findings have informed the appropriations process for the US military, and as such, the National Defense Authorization Act (NDAA) bars the use of Huawei and ZTE equipment for military communications as well as products by Hytera, Hangzhou Hikvision, and Dahua for video surveillance.[8] The House findings are corroborated by the recent Senate Committee on Homeland Security & Government Affairs, Permanent Subcommittee on Investigation's "Majority and Minority Staff Report - Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers."[9]

In any case, there are many Chinese government owned and affiliated firms beyond Huawei operating in the US today which the FCC and Team Telecom need to be concerned about.

[6] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542820
[7] https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96
[8] https://www.congress.gov/bill/115th-congress/house-bill/5515/text
[9] https://www.hsgac.senate.gov/subcommittees/investigations/hearings/majority-and-minority-staff-report_-threats-to-us-networks-oversight-of-chinese-government-owned-carriers

Importance of FCC's focus on security and the implementation of its recent policy to address state-sponsored cyber threats

In November 2019, The FCC adopted the timely and necessary Order Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs.[10] Importantly the Order restricts Universal Service Fund monies for products and services from Huawei Technologies and ZTE. The Order further instructs the identification and restriction of USF monies to other companies posing a national security threat to the integrity of communications networks or the communications supply chain. These efforts have been important for the rollout of secure 5G technologies.

Importantly, the FCC denied a license to China Mobile,[11] and based upon Team Telecom's recommendation, the FCC further investigates China Telecom Americas, China Unicom Americas, Pacific Networks, and ComNet.[12] The Department of Justice (DOJ) through its recent China Initiative focusing on identifying and prosecuting economic espionage, trade secret theft, hacking & other economic crimes.[13] After some years of relative disinterest in China's economic crimes against the US, the DOJ has brought some 50 cases in the last two years alone.[14]

Recently the FCC concluded an Order to make 1200 MHz available in the 6 GHz band for unlicensed use, quintupling the spectrum available for technologies like Wi-Fi.[15] However, the FCC published no plan for whether or how it intends to prevent and deter malicious vendors and vulnerable devices from being deployed in the band. It is not clear that the current order allows a device to be recalled for security reasons. Presently it appears that the FCC only regulates power levels for devices on unlicensed networks.

While the value of Wi-Fi is undisputed, the FCC's 6 GHz Order would seem to give Chinese government owned and affiliated firms free rein to a wide swath of spectrum. Indeed the situation is further heightened as providers of critical infrastructure services in public safety, communications, rail, electric, gas, water, and wastewater operate some 100,000 fixed service links in the band, over which the forthcoming Wi-Fi devices would be deployed, creating not only questions of interference but security.

Meanwhile the 6 GHz Order was celebrated by the Austin, TX Wi-Fi Alliance as "a monumental ruling securing Wi-Fi innovation for decades to come,"[16] ostensibly because the Wi-Fi equipment industry plans to deploy hundreds of millions of devices in the band. Among the 800 members of the Wi-Fi Alliance are many firms owned and affiliated with the Chinese government. These are listed in the US National Vulnerabilities Database, including Huawei which the Wi-Fi Alliance honored as top tier member for its leadership in the Wi-Fi CERTIFIED™ program, allowing its products to be embossed with the Wi-Fi CERTIFIED™ seal.[17] Huawei touts its role in Wi-Fi 6, considered the future-proofing strategy for

[10] https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0
[11] https://www.forbes.com/sites/roslynlayton/2019/04/23/fcc-right-to-reject-state-owned-china-mobile-claim-that-its-not-influenced-by-the-prc/#10b09d523a56
[12] https://www.fcc.gov/document/fcc-scrutinizes-four-chinese-government-controlled-telecom-entities
[13] https://www.justice.gov/opa/gallery/china-initiative-conference
[14] https://www.justice.gov/opa/page/file/1223496/download
[15] https://www.fcc.gov/document/fcc-opens-6-ghz-band-wi-fi-and-other-unlicensed-uses-0
[16] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-delivers-more-value-from-wi-fi-in-6-ghz
[17] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-honors-wi-fi-certified-leaders

the Wi-Fi industry.[18] Other notable members include ZTE Corporation (network equipment) and Hangzhou Hikvision Digital Technology Co., Ltd. (surveillance cameras), firms like Huawei which restricted in the NDAA. Other members with Chinese government ownership and affiliation include Lenovo, Lexmark, TCL Corporation, Panda Electronics, Skyworth, SVA, TCL, Xiaomi, BOE, Changhong, Haier, Hisense, Konka, and DJI.

It is illogical and inconsistent that there is consequential federal policy to make 5G safe from Huawei and ZTE buts allows the same and similar dangerous Chinese government-owned and affiliated firms to roam free on America's Wi-Fi networks and to proliferate across its industry associations which lobby federal officials. Indeed China's influence on standards organizations to circumvent security policy is an established area of policy research.[19] Following placement on the Entity List,[20] Huawei was ejected[21] but then quickly reinstated as a member at the Wi-Fi Alliance,[22] IEEE,[23] SD Association,[24] and JEDEC.[25] Some claim there is no choice but to accept Chinese government owned vendors in standards groups, but China's endgame is clear: It has long been architecting an alternative version of the internet which does not include American technology nor any pretense of coexistence.[26]

In any event, the FCC should use its authority from the Team Telecom Order to scrutinize, reject, and revoke applications from Chinese government owned firms. If the FCC cannot police these firms, it should explore adopting mandatory disclosures for Chinese government owned firms. For example, devices which meet the power transmission requirements display the FCC symbol. One addition could be the embossing of a symbol on the device (or an applied sticker on the product box) noting that the product presents a security risk because its maker is Chinese government owned. Presently there is no federal "Do Not Buy" list for consumers, a user-friendly way to help consumers make informed decisions about their privacy and security when it comes to Chinese-made devices.

The FCC has tools to improve Wi-Fi security, and it should use them.

Role of FCC's spectrum policy to security

The FCC choose to make 1200 MHz of spectrum available for unlicensed technology while the US is behind on making mid-band spectrum available for 5G. China has some 500 MHz of mid-band spectrum in play for 5G and has deployed some 160,000 5G base-stations in 50 cities.[27] The US hasn't even concluded its mid-band 5G auctions, itself a national security issue The US must wait until December for

[18] https://e.huawei.com/en/products/enterprise-networking/wlan/wifi-6/industry-white-paper
[19] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427372
[20] https://www.aei.org/technology-and-innovation/white-house-and-commerce-department-put-chinas-tech-sector-on-notice/
[21] https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-s-voice-in-future-tech-standards-restricted
[22] https://www.techarp.com/mobile/huawei-wifi-alliance-suspension/
[23] https://techcrunch.com/2019/06/02/ieee-lifts-huawei-curbs/?guccounter=2&guce_referrer=aHR0cHM6Ly9jb25zZW50LnlhaG9vLmNvbS8&guce_referrer_sig=AQAAAIZTMdi1qL-PJ3wX01syz3-Ui4TG_YrsHkTIrPZ0h460D7qIBvqXI6HCRF5z8Bcr7xApuhAAY8USWEYHtWDtLcphBjphqt4XW4NL5xeIDPA8j-OMh0IXjIPdb8zjriff4hR_sStUVSgCtRY4O9wRZtrG0TtUiT-mSdFVah4dFpK_
[24] https://www.androidauthority.com/huawei-sd-association-991853/
[25] https://www.androidpolice.com/2019/05/29/huawei-ejected-from-wi-fi-alliance-sd-association-and-other-standards-groups/
[26] https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2
[27] https://www.eetimes.com/5g-wait-til-next-year/

the C-band auction of 250 MHz and yet another year thereafter to repack the spectrum, a slow pace which is itself a national security concern raised by two dozen security and defense experts.[28] As the COVID-19 pandemic has shown, networks were needed yesterday.

The decision to make so much spectrum available for unlicensed network technologies is misguided from a security perspective. As I describe in a forthcoming article in *AGL Magazine* with David Witkowski,[29] 5G networks are inherently safer because of superior architecture. Wi-Fi is ideal for *local* area networks and enterprise deployments in office buildings. 4G LTE and 5G NR, on the other hand, are suited to *wide* area networks and infrastructure deployments which require connection management to ensure reliability and predictably for millions of users at once. These differences reflect the economic choices inherent in licensed and unlicensed spectrum. 5G providers, having spent billions of dollars to purchase the right to transmit data across the airwaves, steward the resource wisely and safely to ensure a good experience for their customers. Unlicensed spectrum, free and open to anyone, has few incentives to be stewarded well. As such, those who value security, pay for it.

Where other users are known, security is less important, and devices can manage their own connections. Users accessing an open, no password required Wi-Fi access point take enormous risks. As Wi-Fi access points grow, it is prudent to adopt rigid security protocols where the network manages the device connection. A connection-oriented or connection-managed protocol (WiMAX, 4G LTE, 5G NR) ***requires*** that an end-to-end data link between the sending node and receiver node be established both before and while data is transferred. Connection-managed protocols have better reliability, predictability, and security because the encryption key exchange is end-to-end and must be completed before data is transferred. In a connection-less protocol, like Wi-Fi, data is sent from the sending node to the network ***without requiring*** an end-to-end link. Users can employ security technologies to protect data from being lost, misrouted, or intercepted, but many threats are managed more efficiently at higher levels in the network. While forthcoming Wi-Fi 6 equipment offers better security, it will take time for every Wi-Fi router to be upgraded, leaving Wi-Fi users at risk in the meantime. With 5G, however, users have built-in advanced security, regardless of the device.

Connection-managed wireless networks such as 4G/5G allow mobility, moving quickly across a large space while keeping a secure, consistent connection. This is provided by a "handoff" system that shifts the connection to the best possible tower or site. On unlicensed, connection-less systems, the client will remain attached to the access point until the connection is so poor that it fails. While some solutions try to make Wi-Fi better, they typically require upfront investment which can add cost to the proffered "free and open" business model. 4G/5G offers patented features to ensure a quality experience: centralized authentication (intelligence in the device ensures network authentication); network rules for security of data transmission; protocols to avoid congestion; spectrum/channel steering, and resource allocation management. 5G security is not perfect – attacks using cellular site equipment (either repurposed or deliberately built to allow state-sponsored surveillance) could harm subscribers, but hacking the firmware of a consumer-grade Wi-Fi access point is a lot easier – and far less expensive – than constructing a cellular site.

[28] https://www.forbes.com/sites/roslynlayton/2020/02/28/national-security-experts-support-fcc-5g-spectrum-plan-voted-today/#6716e5444be6

[29] David Witkowski is Founder & CEO of Oku Solutions LLC and author of Bridging the Gap – 21st Century Telecommunications Handbook. https://jointventure.org/images/stories/pdf/JVSV_Wireless-Telecommunications-Handbook_2ndEd_DEC2019.pdf

As such network design has important security implications. Had the FCC focused on making 5G networks available, it could have avoided many of the security vulnerabilities it must now address with unlicensed technologies on 6 GHz.