LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, JULY 13, 2020

PERSPECTIVE

FCC designates Huawei as national security threat

By Janice W. Reicher and Hilary C. Krase

New York Times News Service

A Huawei billboard in Shanghai, China, May 28, 2019.

In the ongoing confrontation between the U.S. government and Chinese telecom giant Huawei, the U.S. has dealt another major blow. The Federal Communications Commission issued an order on June 30, effective immediately, declaring that "funds from the Commission's Universal Service Fund [(USF)] may no longer be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by Huawei." The commission determined that Huawei is a national security threat based on the "totality of the evidence" surrounding the company. The $8.3 billion per year USF provides federal funds to telecommunications providers through different mechanisms to make such services affordable to residents in certain high-cost regions, low-income customers, rural health care providers, and eligible schools and libraries.

The U.S. government's assertion that Huawei poses a national security threat is not new. The federal government has repeatedly taken actions against Huawei based on national security and espionage concerns, which Huawei has vehemently opposed. In 2012, a U.S. House of Representatives Intelligence Committee Report deemed Huawei a national security threat and recommended that the U.S. government telecommunication systems not include equipment from Huawei or fellow Chinese multinational telecommunications company ZTE Corporation. The Report cited, among other things, an "ongoing onslaught of sophisticated computer network intrusions that originate in China, and are almost certainly the work of, or have the backing of, the Chinese government," as well as evidence that "Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data."

In August 2018, The Trump administration banned the use of Huawei and ZTE technology by the U.S. government and its contractors as part of the Defense Authorization Act. Then in November 2018, the Department of Justice announced its "China Initiative," designed to "identify priority Chinese trade theft cases, ensure that we have enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively," though it did not call out Huawei specifically in its announcement. In May 2019, the Commerce Department placed Huawei on its Entity List, restricting the sale or transfer of American technology to the company and concluding that Huawei was engaged in activities contrary to U.S. national security or foreign policy interests; this followed President Donald Trump's executive order prohibiting transactions involving information and communications technology provided by companies subject to the jurisdiction or direction of a foreign adversary where the transaction would pose a threat to national security.

Lead up to the Commission's June 30 Order

In November 2019, the FCC adopted the Protecting Against National Security Threats Order, which prohibited the "use of universal service support to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply." The FCC initially designated Huawei and ZTE Corporation as companies covered by this rule and opened a 30-day period for interested parties to file comments, which Huawei did, challenging the designation.

More recently, in March 2020, President Trump signed into law the Secure and Trusted Communications Networks Act of 2019, which directed the FCC to publish a list of covered equipment or services that present an improper threat to national security and bans the use of federal subsidized funds to obtain or maintain such equipment or services. The list encompassed equipment produced by Huawei, its subsidiaries, and its affiliates. As interpreted by the commission, section 3 of the Secure Networks Act instructed the commission to "implement" a ban on the use of USF monies for covered services and

equipment from listed entities including Huawei.

The Commission's Order

The FCC's June 30 order was the final act cementing Huawei's ban from accessing USF funds. The order was driven, in part, by the need to "protect[] and secur[e] communications infrastructure and the supply chain from Huawei" which poses a national security risk. The commission highlighted several pieces of evidence supporting its findings. In particular, the commission found that Huawei is highly susceptible to coercion, in part, because of its close ties to the Chinese government and military at the ownership and employee level. Furthermore, the commission found that the Chinese National Intelligence Law compels Huawei "to assist the Chinese government in espionage activities." The commission continued, stating that, broadly applied, the law could reasonably allow the Chinese government to require Huawei's U.S. subsidiary to "carry out its directives in cyberespionage[.]"

The commission also determined that its findings aligned with actions taken by Congress, the executive branch, policymakers, and the intelligence community, among others. For example, while the European Union has not explicitly banned Huawei from is 5G networks, it has issued guidelines for vetting vendors and permits EU capitals to limit Huawei's role in the networks because Huawei may pose a threat to its security as a result of influence and coercion by the Chinese government. Furthermore, the commission cited evidence that Huawei's equipment contains known security risks and vulnerabilities, as articulated in a 2019 report by cybersecurity firm Finite State.

Huawei responded, in part, that all companies operating in China must maintain internal Communist Party committees, which the commission did not find reassuring. Furthermore, Huawei asserted that the Chinese National Intelligence law does not allow the Chinese government to require Huawei to engage in espionage. The commission dismissed Huawei's narrow interpretation in part because of Huawei's close connection to the Chinese government and the risk of collaboration.

Implications of FCC Ban

The order, which applies not only to Huawei but also to its parents, affiliates, and subsidiaries, poses a serious threat to Huawei's efforts to expand its 5G network globally. Other countries are apparently taking notice of the U.S. government's findings against Huawei. For example, the week after the commission issued its order, UK Prime Minister Boris Johnson signaled that the British government may be reconsidering its stance on Huawei and may further limit the company's role in building Britain's 5G mobile phone network.

In the U.S., the order also has implications for access to telecommunications services and equipment, particularly in rural areas. Although the FCC reported that Huawei equipment only makes up a small percentage of equipment in U.S. networks, the Rural Wireless Association, Inc. (RWA), a trade group representing small internet service providers, estimated that 25% of its members used either Huawei or ZTE in their networks. The RWA previously expressed concern over the designations absent reimbursement funding to replace covered equipment. On June 30, 2020, RWA released a statement in response to the commission's order, stating that it was "stunned" by the decision. "As a result, rural carriers who have deployed Huawei or ZTE equipment or services in their networks will now lack the ability to support their critical networks that are serving hundreds of thousands of rural Americans and those traveling through rural America."

The Future for U.S.-China and Huawei Relations

As Huawei competes to dominate the future of 5G telecommunications, the U.S. government's scrutiny of the company could not be more acute. With the upcoming November presidential election, there is speculation as to what approach a potential Biden Administration might take towards U.S.-China relations and companies like Huawei. Although the answer is still unknown, there are indications that a change in administration would not mean a softened U.S. stance towards China. Joe Biden has recently made comments regarding the perceived threat China poses, including from "cyber-theft" and "other predatory practices," and suggested that he would take a firm stance against China and its state-owned enterprises. For now, the FCC's latest decision imposes a major obstacle for Huawei in its efforts to increase its presence in 5G networks in the United States. ■

Janice W. Reicher *is co-chair of Farella Braun + Martel's White Collar Defense and Internal Corporate Investigations Group and a member of its Business Litigation Group in the San Francisco office. She represents individuals and entities in high-profile criminal and parallel civil matters.*

Hilary C. Krase *is a member of Farella Braun + Martel's White Collar Defense and Internal Corporate Investigations Group as well as the Business Litigation Group. She represents individuals and entities in civil matters in both federal and state court and counsels individuals in a variety of criminal matters.*