United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
June 18, 2021
Lyle W. Cayce
Clerk

No. 19-60896

HUAWEI TECHNOLOGIES USA, INCORPORATED; HUAWEI TECHNOLOGIES COMPANY, LIMITED,

Petitioners,

versus

FEDERAL COMMUNICATIONS COMMISSION; UNITED STATES OF AMERICA,

Respondents.

On Petition for Review of an Order of the
Federal Communications Commission, No. 19-121

Before ELROD, DUNCAN, and WILSON, *Circuit Judges*.

STUART KYLE DUNCAN, *Circuit Judge*:

An FCC rule bars using government subsidies to buy equipment from companies designated security risks to communications networks. *See* Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 85 Fed. Reg. 230-01 (Jan. 3, 2020). We consider a challenge to that rule by Huawei Technologies Company and its American affiliate, Huawei Technologies USA.

INTRODUCTION

The federal government annually distributes billions of dollars to promote telephone and Internet service across our nation. These subsidies, called "universal service funds," are administered by the Federal Communications Commission ("FCC"). Last year, that agency issued a rule barring recipients from using the funds to buy equipment or services from companies designated "national security risks" to communications networks and supply chains. Under the rule, the FCC designated Huawei, a Chinese telecom provider, and its American affiliate as national security risks. The companies now level myriad challenges, both statutory and constitutional, to the rule and to their designation.

Their most troubling challenge is that the rule illegally arrogates to the FCC the power to make judgments about national security that lie outside the agency's authority and expertise. That claim gives us pause. The FCC deals with national communications, not foreign relations. It is not the Department of Defense, or the National Security Agency, or the President. If we were convinced that the FCC is here acting as "a sort of junior-varsity [State Department]," *Mistretta v. United States*, 488 U.S. 361, 427 (1989) (Scalia, J., dissenting), we would set the rule aside.

But no such skullduggery is afoot. Assessing security risks to telecom networks falls in the FCC's wheelhouse. And the agency's judgments about national security receive robust input from other expert agencies and officials. We are therefore persuaded that, in crafting the rule, the agency reasonably acted within the broad authority Congress gave it to regulate communications. Additionally, having carefully considered the companies' other challenges under the Administrative Procedure Act and the Constitution, we find those unavailing as well.

We therefore deny the petition for review.

Table of Contents

BACKGROUND

Huawei Technologies Company ("Huawei") is a global provider of telecommunications equipment and services established and headquartered in China. It supplies smart device, cloud, and 5G broadband cellular technology to commercial entities and consumers. Huawei-USA launched in 2001 and maintains its U.S. headquarters in Plano, Texas.

As early as 2011, Huawei began attracting the U.S. government's attention as a potential security risk to American telecommunications networks.[1] In October 2012, the U.S. House Permanent Select Committee on Intelligence ("HPSCI") published a report finding, "Huawei . . . cannot be trusted to be free of foreign state influence and thus pose[s] a security threat to the United States and to our systems." *HPSCI Report*, at vi–vii. The HPSCI admonished U.S. government systems operators and contractors to exclude Huawei equipment and encouraged private entities to reconsider Huawei-associated security risks and "seek other vendors." *Id.* at vi.

In late 2017, members of Congress expressed apprehension about "Chinese espionage" and "Huawei's role in [it]" to then-Chairman of the FCC, Ajit Pai.[2] Pai's reply conveyed "share[d] . . . concerns about the security threat that Huawei and other Chinese technology companies pose to our communications networks."[3] He promised "to take proactive steps" to

---

[1] MIKE ROGERS & C.A. DUTCH RUPPERSBERGER, HPSCI, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE iv (2012), https://tinyurl.com/yyp5muou [hereinafter *HPSCI Report*].

[2] Letter from Tom Cotton et al., Members, U.S. Congr., to Ajit Pai, Chairman & Commiss'r, FCC (Dec. 20, 2017), https://tinyurl.com/yx6xp217.

[3] Letter from Ajit Pai, Chairman, FCC, to Tom Cotton, Sen., U.S. S. (Mar. 20, 2018), https://tinyurl.com/u2verd9.

"ensure the integrity of the communications supply chain . . . in the near future." *Id.*

Around this time, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2018 ("2018 NDAA"), which barred the Defense Department from procuring telecommunications equipment produced by Huawei.[4] The 2019 NDAA went further, prohibiting all executive agencies from obtaining Huawei equipment, contracting with entities that use it, or using loan or grant funds to obtain it.[5] Sharing these concerns, then-President Donald Trump issued executive orders addressing the issue in 2019 and 2020.[6]

Against this backdrop, the FCC issued an April 2018 notice of proposed rulemaking ("NPRM"), "In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs."[7] The notice concerned "universal service funds" (or "USF funds"), a pool of money the FCC dispenses to certain providers to promote "universal service." *See* 47 U.S.C. § 254(e); *see also Alenco Commc'ns, Inc. v. FCC*, 201 F.3d 608, 617 (5th Cir. 2000).[8] USF funds foster affordable telephone and internet access in high-cost areas, subsidize rates

---

[4] *See* Pub. L. No. 115-91, § 1656(b)(1), (c)(3)(A), 131 Stat. 1283, 1762 (2017).

[5] *See* Pub. L. No. 115-232, § 889(a)–(b), (f)(3)(A), 132 Stat. 1636, 1917–18 (2018).

[6] Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 15, 2019); Exec. Order No. 13913, 85 Fed. Reg. 19,643 (Apr. 4, 2020).

[7] Notice of Proposed Rulemaking in the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs ("Supply Chain Rulemaking"), FCC 18-42, WC Docket No. 18-89, 33 FCC Rcd. 4058 (released Apr. 18, 2018).

[8] Universal service is defined as "an evolving level of telecommunications services that the Commission shall establish periodically . . . , taking into account advances in telecommunications and information technologies and services." § 254(c)(1).

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.