United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued September 20, 2022 Decided August 15, 2023

No. 22-1054

PACIFIC NETWORKS CORP. AND COMNET (USA) LLC,
PETITIONERS

v.

FEDERAL COMMUNICATIONS COMMISSION AND UNITED STATES OF AMERICA,
RESPONDENTS

On Petition for Review of an Order
of the Federal Communications Commission

Christopher J. Wright argued the cause for petitioners. With him on the joint briefs were *Jeffrey Carlisle* and *Stephen Coran*.

Scott M. Noveck, Counsel, Federal Communications Commission, argued the cause for respondents. With him on the brief were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, U.S. Department of Justice, *Sharon Swingle* and *Casen Ross*, Attorneys, and *Jacob M. Lewis*, Deputy General Counsel, Federal Communications Commission.

Before: HENDERSON and KATSAS, *Circuit Judges*, and EDWARDS, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* KATSAS.

KATSAS, *Circuit Judge*: Pacific Networks Corp. and ComNet (USA) LLC, which are companies owned by the People's Republic of China, held authorizations to operate communication lines in the United States. The Federal Communications Commission revoked these authorizations based on concerns that the carriers posed national-security risks and had proven themselves untrustworthy. The carriers argue that the FCC's reasoning was substantively arbitrary and was rendered with inadequate process. We reject both contentions.

I

A

Section 214(a) of the Communications Act of 1934 makes it unlawful to operate any wire communications line without authorization from the FCC. 47 U.S.C. § 214(a). In deciding whether to grant such authorization, the Commission considers the "public convenience and necessity," *id.*, including whether authorization would imperil "the national defense," *id.* § 151. In assessing national-security risks posed by foreign-owned companies, the FCC has long consulted other federal agencies with expertise in that area. *See Rules and Policies on Foreign Participation in the U.S. Telecomms. Mkt.*, 12 FCC Rcd. 23,891, 23,919–22 (1997). This group of agencies is known colloquially as Team Telecom.

A recent executive order formalized this process by establishing a committee "to assist the FCC in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunication services sector." Exec. Order No. 13913, § 3(a), 85 Fed. Reg. 19,643, 19,643 (Apr. 4, 2020). The

committee includes the Secretary of Homeland Security, the Attorney General, and the Secretary of Defense. *Id.* § 3(b), 85 Fed. Reg. at 19,643–44.

B

In recent years, the United States has grown increasingly concerned about espionage and other threats from Chinese-owned telecommunications companies.

In 2018, Team Telecom recommended that the FCC deny a section 214 authorization to one such company, China Mobile International (USA) Inc. Team Telecom concluded that the proposed authorization "would pose substantial and unacceptable national security and law enforcement risks" because the company's ownership made it "subject to exploitation, influence, and control by the Chinese government." *Redacted Exec. Branch Recommendation to the FCC to Deny China Mobile International (USA) Inc.'s Application for an Int'l Section 214 Authorization*, FCC No. ITC-214-20110901-00289, at 7 (July 2, 2018) (*China Mobile Recommendation*). The FCC agreed and denied the requested authorization on that basis. *China Mobile Int'l (USA) Inc.*, 34 FCC Rcd. 3361, 3365–66 (2019).

Invoking the same concerns, the FCC later revoked section 214(a) authorizations held by another Chinese-owned carrier, China Telecom (Americas) Corp. *China Telecom (Americas) Corp.*, 36 FCC Rcd. 15,966, 15,992 (2021). We denied a petition for review in that case. *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2022).

C

Through a web of foreign affiliates, China also owns a controlling interest in Pacific Networks and its wholly owned

subsidiary, ComNet. Until 2022, these companies held section 214(a) authorizations. Pacific Networks provided business networking services extending internationally, while ComNet sold international calling cards. To obtain their authorizations, the carriers promised to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. records." J.A. 21.

In 2020, the FCC ordered Pacific Networks and ComNet to show cause why their authorizations should not be revoked. *Pac. Networks Corp.*, 35 FCC Rcd. 3733 (2020). Citing its *China Mobile* order, the Commission questioned whether Pacific Networks and ComNet, as companies indirectly owned by China, would be subject to its "exploitation, influence, and control." *Id.* at 3735–36. The carriers submitted a 37-page response with hundreds of pages of exhibits.

Team Telecom then weighed in. It concluded that China's ownership raised "significant concerns" that the carriers would be "forced to comply with Chinese government requests, including requests for communications intercepts." J.A. 114. Likewise, the carriers could be "exploit[ed] by the Chinese government … to conduct or to increase economic espionage and collect intelligence against the United States." *Id.* at 116.

In 2021, the FCC instituted a full proceeding to consider revoking the authorizations. *Pac. Networks Corp.*, 36 FCC Rcd. 6368 (2021). It identified various open issues. This time around, the carriers submitted an 84-page response with hundreds of pages of exhibits.

The FCC revoked the authorizations. It concluded that "ownership and control by the Chinese government raise significant national security and law enforcement risks by providing opportunities for the [carriers], their parent entities and affiliates, and the Chinese government to access, monitor,

store, and in some cases disrupt [or] misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States." *Pac. Networks Corp.*, FCC 22-22, 2022 WL 905270, at *1 (FCC Mar. 23, 2022) (*Revocation Order*). The Commission further concluded that the carriers had shown a lack of candor and trustworthiness. And for both reasons, it concluded that nothing short of revocation would ameliorate the national-security risks.

The carriers petitioned this Court for review. We have jurisdiction under 28 U.S.C. § 2342(1) and 47 U.S.C. § 402(a).

II

Under the Administrative Procedure Act, we must consider whether the *Revocation Order* was arbitrary or capricious. 5 U.S.C. § 706(2)(A). This "deferential" standard requires only "that agency action be reasonable and reasonably explained." *FCC v. Prometheus Radio Project*, 141 S. Ct. 1150, 1158 (2021). Pacific Networks and ComNet assert that the FCC arbitrarily assessed national security, candor, and mitigation. We address each consideration in turn.

A

The carriers contend that the FCC unreasonably found a threat to national security. But the Commission meticulously explained—over the span of 62 pages—how the carriers' domestic operations threaten national security. First, the agency described how China holds a majority interest in Pacific Networks and ComNet through various affiliated Chinese companies, which exercise significant control over the carriers' day-to-day operations. *Revocation Order* at *18–20, *24–25. Next, it detailed how China can access the carriers' records through those affiliates, *id.* at *24, including by invoking a

Chinese law requiring all Chinese corporations to "support, assist, and cooperate with national intelligence efforts," *id.* at *30 (quotation omitted). Finally, it explained the breadth and sensitivity of the carrier records: ComNet has amassed detailed call records of its United States customers, including numbers called as well as the frequency, duration, and timing of the calls. *Id.* at *38. Furthermore, it can monitor the calls themselves. *Id.* Pacific Networks likewise can "access, monitor, store, [or] disrupt" communications sent over its networks, and it has access to customers' personally identifiable information. *Id.* at *40.

We cannot second-guess the FCC's judgment that allowing China to access this information poses a threat to national security. In making it a crime to obtain call records without authorization, Congress found that "call logs may include a wealth of personal data" about a person's business, medical records, private relationships, and more. Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, § 2, 120 Stat. 3568, 3568; *see* 18 U.S.C. § 1039(a). Courts likewise have observed that call records often contain a "startling amount of detailed information," such as whether an individual is "a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime." *ACLU v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015). China has exploited such information—like the fact that a former United States intelligence officer was having financial difficulties—to recruit spies. *See United States v. Mallory*, 40 F.4th 166, 169–71 (4th Cir. 2022). More generally, Team Telecom has warned that China uses information obtained from telecommunications carriers—including but not limited to call records—"to conduct or to increase economic espionage and collect intelligence against the United States." J.A. 116.

The carriers do not seriously contest any of this. Instead, they fault the FCC for even considering whether their operations could facilitate Chinese espionage. According to the carriers, the Commission should have focused solely on whether they posed a threat to domestic telecommunications infrastructure. As the carriers note, Team Telecom often has focused on that specific threat. But it also considers more generally whether carriers engage in "activities with potential national security implications." *China Mobile Recommendation*, FCC No. ITC-214-20110901-00289, at 6–7. In any event, the licensing decision is vested in the FCC, which must consider both "the national defense," 47 U.S.C. § 151, and the "public convenience and necessity," *id.* § 214(a). These factors plainly encompass the question whether authorizations would facilitate espionage.

The carriers further note that Team Telecom declined to recommend revocation in this case. But that was because the FCC asked it to answer discrete questions within a "limited time" of one month. J.A. 109. Moreover, Team Telecom did not recommend against revocation, and it did note that the operations of Pacific Networks and ComNet posed similar national-security risks to the ones detailed more fully in its *China Mobile Recommendation*. J.A. 116. Finally, when the FCC received Team Telecom's input in this case, it did not reflexively revoke, but instead set the matter for full written submissions. None of this was arbitrary.

In sum, the FCC reasonably concluded that the domestic operations of ComNet and Pacific Networks threatened national security by making vast amounts of sensitive information easily available to China.

B

The carriers also challenge the FCC's determination that they lacked candor and trustworthiness. But the agency amply justified its concern. *Revocation Order*, 2022 WL 905270, at *49–60. To begin with, the FCC explained how the carriers gave misleading and incomplete responses to the show-cause order. Despite being asked to identify the senior management of every entity that held a 10% or greater direct or indirect interest in Pacific Networks, the carriers provided information only for the direct parent company of Pacific Networks. Response to Order to Show Cause, FCC No. ITC-214-20090105-00006, at 11–12 & Ex. A-1 (filed June 1, 2020). And they submitted an ownership chart not disclosing the Chinese government at all. *Revocation Order*, 2022 WL 905270, at *52.

The FCC also explained how the carriers downplayed China's control over their operations. For example, while the carriers represented that they operated "independently" of their foreign affiliates, the Commission's investigation showed that one affiliate played "an integrated role" in their operations, including by managing access to their United States customer records. *Revocation Order*, 2022 WL 905270, at *53, *55. And during a Senate investigation into how Chinese-owned carriers threaten national security, ComNet stated that "its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems." Staff of Permanent Subcomm. on Investigations of the S. Comm. on Homeland Sec. & Governmental Affs., 116th Cong., Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers 96 (2020). But evidence before the FCC showed that China can access both ComNet's records and data that passes through its facilities. *Revocation Order*, 2022 WL 905270, at *43.

Again, the carriers do not seriously contest the FCC's factual determinations. Instead, they object that the Commission had never revoked a section 214 authorization based solely on misrepresentations. The carriers cite past cases where concerns about candor or trustworthiness produced only a fine. *See, e.g.*, *Omniat Int'l Telecom, LLC*, 24 FCC Rcd. 4254 (2009); *Skyport Glob. Commc'ns, Inc.*, 24 FCC Rcd. 3714 (2009). But those cases did not involve national-security risks, which plainly heighten any trustworthiness concerns.

C

Finally, Pacific Networks and ComNet claim that the FCC arbitrarily rejected the possibility of mitigating measures short of revocation. But the Commission explained its view that the carriers' untrustworthiness would make any mitigation agreement too risky: Such agreements are not self-enforcing, and the agency cannot comprehensively monitor compliance. *Revocation Order*, 2022 WL 905270, at *66. Furthermore, oversight cannot reliably detect surreptitious, state-sponsored efforts at evasion. *Id.* In short, the FCC reasonably explained why no realistic agreement could have worked given the carriers' proven lack of trustworthiness.

III

Pacific Networks and ComNet also challenge the process underlying the FCC's decision. The carriers primarily contend that the Due Process Clause and the APA require the agency, before it may revoke a section 214(a) authorization, to hold a live evidentiary hearing before a neutral adjudicator with an opportunity for discovery and cross-examination. We rejected that argument in *China Telecom*. *See* 57 F.4th at 268–71.

The carriers conclude with a hodgepodge of further procedural objections. They say that the FCC imposed the

burden of proof on them, failed to acknowledge disputed material facts, proceeded without a formal recommendation from Team Telecom, and proceeded by adjudication rather than by rulemaking. None of these further claims has merit. As detailed above, the FCC amply proved facts establishing both a national-security risk and a lack of trustworthiness. Nothing in the Due Process Clause, the APA, or the Communications Act requires the Commission to consult with other agencies, which it did in any event. And nothing in these laws required it to proceed by rulemaking in assessing the specific risks posed by these individual carriers. *See NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974).

IV

The FCC adequately explained its decision to revoke Pacific Networks' and ComNet's authorizations, and it afforded adequate process to the carriers. We therefore deny the petition for review.

So ordered.