

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,

Petitioner,

v.

CHINA TELECOM (AMERICAS)
CORPORATION,

Respondent.

Filed with the Classified
Information Security Officer

CISO

Date

9/2/2021

No. 20-mc-116 (DLF)

MEMORANDUM OPINION AND ORDER

Before this Court is the United States's Petition to Initiate a Determination That Certain FISA Surveillance Was Lawfully Authorized and Conducted, Dkt. 1. The United States requests a judgment that its electronic surveillance authorized under the Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (1978), was lawful because it intends to use said information in a proceeding against respondent China Telecom (Americas) Corporation (CTAC) before the Federal Communications Commission (FCC). Gov't's Pet. at 1. For the reasons that follow, the Court will grant the United States's petition and enter a judgment that the surveillance was lawfully authorized and collected.

I. BACKGROUND

A. Statutory

FISA is the statutory scheme by which the Executive Branch conducts electronic surveillance and physical searches to obtain foreign intelligence information (FII). The government begins by filing an *ex parte* application to authorize electronic surveillance before

the Foreign Intelligence Surveillance Court (FISC). 50 U.S.C. §§ 1803(a), 1805(a). In that application, the government must:

- (1) identify “the Federal officer making the application;”
- (2) identify or describe “the specific target of the electronic surveillance”
- (3) justify with “facts and circumstances” the belief that the target “is a foreign power or an agent” thereof, and the facilities targeted are “being used, or [are] about to be used by a foreign power or an agent” thereof;
- (4) provide “a statement of the proposed minimization procedures;”
- (5) provide “a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;”
- (6) provide “a certification or certifications by” appropriate national security officials—
 - (A) “that the certifying official deems the information sought to be” FII;
 - (B) “that a significant purpose of the surveillance is to obtain” FII;
 - (C) “that such information cannot reasonably be obtained by normal investigative techniques;”
 - (D) “that designates the type of” FII pursued; and
 - (E) “including a statement of the basis for the certification that—
 - (i) “the information sought is the type of [FII] designated;” and
 - (ii) “such information cannot reasonably be obtained by normal investigative techniques;”
- (7) summarize how “the surveillance will be effected and . . . whether physical entry is required to effect the surveillance;”

(8) state “the facts concerning all previous [FISA] applications. . . involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;” and

(9) state the proposed duration of surveillance.

Id. § 1804(a)(1)–(9). After review of such an application, a district judge appointed to FISC pursuant to 50 U.S.C. § 1803(a)(1) “shall enter an *ex parte* order” after making the following findings:

(1) “the application has been made by a Federal officer and approved by the Attorney General;”

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the surveillance target “is a foreign power or an agent of a foreign power” except that “no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of” First Amendment-protected activities; and

(B) each targeted facilities is or soon will be used “by a foreign power or an agent” thereof;

(3) the proposed minimization procedures meet the” statutory definition; and

(4) the application contains all required statements and certifications “and, if the target is a United States person, the certifications are not clearly erroneous”

Id. § 1805(a)(1)–(4).

Before the United States uses information collected under a FISA surveillance order in any kind of proceeding against an aggrieved person, the government must provide that person

advance notification. *Id.* § 1806(c). To determine the legality of the surveillance while protecting national security, district courts “shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” *Id.* § 1806(f). In conducting this review, the court “may disclose” FISA application materials “only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” *Id.*

B. Factual and Procedural

This petition arises out of proceedings before the FCC to revoke CTAC’s license under § 214 of the Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064. *See* Pet. at 1–2. In 2007, CTAC received a license “to provide telecommunications services domestically and between the United States and foreign countries as a licensed international common carrier.” *Id.* at 2. In 2020, several federal agencies recommended that the FCC revoke CTAC’s license because of national security concerns and “failure to adhere to the conditions of its” license. *Id.* (citing *In the Matter of China Telecom (Americas) Corp.*, FCC File Nos. ITC-214-20010613-00346; ITC-214-20020716-00371; ITC-T/C-20070725-00285, at 56 (filed Apr. 9, 2020) (hereinafter “Recommendation”). The Department of Justice notified CTAC that it intended to file classified FISA information *ex parte* with the FCC. *Id.* at 3.

On April 20, 2020, the FCC ordered CTAC to show cause why it “should not initiate a proceeding to revoke CTAC’s 214 authorizations.” *Id.* CTAC responded to this on the merits and requested access to the government’s FISA submissions. *Id.* The company claimed that this was to “preserve its fundamental due process rights” and “to determine whether there are

grounds to seek suppression of those materials.” *Id.* at 4. In November 2020, the government instituted these proceedings to obtain a determination of legality. *See id.* at 11.

II. LEGAL STANDARD

This Court reviews *de novo* the government’s application for probable cause. *See In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 204–05 (7th Cir. 2003); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 311 (D. Conn. 2008), *aff’d*, 630 F.3d 102 (2d Cir. 2010). The government must show that “there is probable cause to believe that . . . ‘the target of the electronic surveillance is . . . an agent of a foreign power’ and that ‘each of the facilities or places at which the electronic surveillance is directed is being used, or about to be used, by . . . an agent of a foreign power.’” *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (en banc) (quoting 50 U.S.C. § 1805(a)(3)) (second and third omission in original), *vacated*, 543 U.S. 1097, *reinstated in relevant part*, 405 F.3d 1034 (2005). In evaluating probable cause, this Court must “make a practical common-sense” judgment that “given all the circumstances set forth in the affidavit . . . , there is a fair probability’ that the search will be fruitful.” *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 232 (1983)) (omission in original). The government’s certifications are entitled to a presumption of validity. *United States v. Mohammad*, 339 F. Supp. 3d 724, 736 (N.D. Ohio 2018); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 131 (D. Mass. 2007); *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006).

III. ANALYSIS

A. CTAC Is Not Entitled to Inspect FISA Materials

The respondent advances statutory and constitutional arguments to support its claim that it is entitled to disclosure of FISA materials. *See* Resp.'s Opposition at 19. All precedent, in and out of this circuit, clearly forecloses disclosure in this case.

Section 1806(f) provides that courts “*may* disclose . . . materials . . . *only* where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance.” 50 U.S.C. § 1806(f) (emphasis added). The D.C. Circuit has explained that such disclosure is “the exception,” not the rule. *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982); *see also United States v. Stewart*, 590 F.3d 93, 127–28 (2d Cir. 2009); *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991). Necessity turns on the presence of such factors as “indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.” *Belfield*, 692 F.2d at 147 (quoting S. Rep. No. 95–701, 95th Cong., 2d Sess. 64 (1978)).

Here, the respondent contends that necessity is present due to factual misrepresentations by the government. *See* Resp.'s Opposition at 19–20. Upon review of the FISA materials, *see supra* section II.C, this Court finds that none of the aforementioned factors are present in this case.

Nor does “due process require[] disclosure” under § 1806(g), *see* Resp.'s Opposition at 27. Section 1806(g) provides that a court reviewing FISA materials *in camera* and *ex parte* under § 1806(f) “shall deny to motion of the aggrieved person except to the extent that due process requires discovery or disclosure.” 50 U.S.C. § 1806(g). CTAC argues that it has a

protected property interest in its FCC license and that due process requires a hearing and an opportunity to respond to evidence against it. *See* Resp.'s Opposition at 27–31. Again, *Belfield* forecloses this argument. The exclusion of aggrieved parties from the review process does not “rise[] to the level of a constitutional violation” because Congress has “balanc[ed] the competing concerns of individual privacy and foreign intelligence” and found that the process prescribed by FISA “reconcile[s] national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.” *Belfield*, 692 F.2d at 148 (quoting S. Rep. No. 95–701 at 16). Other courts have come to the same conclusion. *See, e.g., United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014) (rejecting the argument “that adversary procedure is always essential to resolve contested issue of fact”); *United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011) (conducting *Mathews* balancing test and concluding that FISA process does not violate defendant’s due process rights); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) (concluding that *ex parte, in camera* review process does not deprive defendant of due process). As such, respondent’s arguments to the contrary fail.

Thus, CTAC is not entitled as a statutory or constitutional matter to disclosure of FISA materials.

B. The Government Filed the Appropriate Certifications

The Court has reviewed the certifications filed by the government and finds that they are all in place. Under 50 U.S.C. § 1806(f), Attorney General William Barr certified that disclosure of the classified documents that support the United States’s petition would harm the national security of the United States. *See* Gov’t’s Mem. in Supp. of Pet. Ex. 1, at 2. [REDACTED]

[REDACTED]

[REDACTED] This Court's *ex parte, in camera* review of the documents has revealed nothing that rebuts "the presumption of validity" that attaches to the government's certifications in these cases.

Also present is the United States's motion to unseal and release certified copies of the warrant application, its supporting document, and the court order for purposes of review by this court. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Upon its review of the documents, the Court finds that all the certifications are in place, are authenticated by the seal of the FISC, and nothing rebuts the presumption of validity that attaches to them.

Finally, the appropriate certifications under 50 U.S.C. § 1804(a)(6) are also in place. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Having reviewed the certification and having found the statutory requirements satisfied, the Court finds nothing to rebut the presumption of validity.

C. The FISA Warrant Applications Were Supported by Probable Cause

Finally, the Court reviews the probable cause determination by the FISC and concludes that there was probable cause for the warrants to issue.

In the review of a warrant application, it is “the duty of the reviewing court . . . to ensure that the magistrate had a substantial basis for . . . concluding probable cause existed.” *United States v. Nozette*, 692 F. Supp. 2d 110, 111 (D.D.C. 2010) (quoting *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983)). The applicant’s affidavit must have “set forth facts sufficient to induce a reasonably prudent person to believe that a search” of the place described in the warrant “will uncover evidence of a crime.” *United States v. Burroughs*, 882 F. Supp. 2d 113, 118 (D.D.C. 2012) (quoting *United States v. Laws*, 808 F.2d 92, 94 (D.C. Cir. 1986)). The government’s FISA warrant application set forth sufficient facts.

[REDACTED]

[REDACTED]

[illegible]

Upon the Court's full review of the record in this petition, the Court is satisfied that the government met its obligations under FISA and established probable cause for its search before the FISC.

CONCLUSION

For the foregoing reasons, this Court finds that United States's FISA surveillance was lawfully authorized and conducted and that the respondent's statutory and due process rights were not violated by an *in camera, ex parte* review as provided by statute. Accordingly, it is

ORDERED that the government's Petition to Initiate a Determination that Certain FISA Surveillance Was Lawfully Authorized and Conducted, Dkt. 1, is **GRANTED**. It is further

ORDERED that the China Telecom (Americas) Corporation's Sealed Motion for Leave to File Document Under Seal, Dkt. 12, is **GRANTED**.

SO ORDERED.


DABNEY L. FRIEDRICH
United States District Judge

September 2, 2021