NO. _____

In The
Supreme Court of the United States

SEITU SULAYMAN KOKAYI,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

Mark J. Petrovich
Counsel of Record
PETROVICH & WALSH, PLC
10605 Judicial Drive, Suite A-5
Fairfax, Virginia 22030
(703) 934-9191
mp@pw-lawfirm.com

Counsel for Petitioner

Anthony H. Nourse
LAW OFFICE OF ANTHONY H. NOURSE, PLC
4151 Chain Bridge Road
Fairfax, Virginia 22030
(703) 881-9161
ahn@fairfaxdefense.com

Counsel for Petitioner

Dated: November 19, 2021

THE LEX GROUP^{DC} ♦ 1050 Connecticut Avenue, N.W. ♦ Suite 500, #5190 ♦ Washington, D.C. 20036
(202) 955-0001 ♦ (800) 856-4419 ♦ www.thelexgroup.com

QUESTION PRESENTED

Whether electronic surveillance undertaken by the United States, of a United States citizen, pursuant to perceived authority under the Foreign Intelligence Surveillance Act ("FISA") can be undertaken and repeatedly reauthorized upon renewed findings of probable cause over a period of years (upon information and belief), without any alleged terrorism or espionage-related charges or substantive changes in circumstances to support the ongoing surveillance, is a violation of FISA, and/or the First and/or Fourth Amendments to the United States Constitution?

PARTIES TO THE PROCEEDINGS

All parties to the proceedings appear in the caption on the cover page.

RELATED CASES

The following proceedings are directly related to this petition:

United States v. Kokayi, No. 19-4510, United States Court of Appeals for the Fourth Circuit, judgment entered August 24, 2021.[1]

United States v. Kokayi, No. 1:18-cr-00410-LMB, United States District Court for the Eastern District of Virginia, Alexandria Division, judgment entered June 28, 2019.[2]

[1] Cert Appendix at 35a

[2] Cert Appendix at 46a

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTIONAL PROVISIONS

STATUTES

RULE

OPINIONS BELOW

There are no opinions below that have been published or that are designated for being published. The unpublished opinions below are as follows.

United States v. Kokayi, No. 19-4510, United States Court of Appeals for the Fourth Circuit, unpublished opinion dated August 24, 2021.[3]

United States v. Kokayi, No. 1:18-cr-00410-LMB, United States District Court for the Eastern District of Virginia, Alexandria Division, memorandum opinion dated July 9, 2019.[4]

JURISDICTION STATEMENT

The district court in the Eastern District of Virginia had jurisdiction over this case pursuant to 18 U.S.C. § 3231. The Court of Appeals for the Fourth Circuit had jurisdiction over Petitioner's Appeal pursuant to 28 U.S.C. § 1291 and Federal Rule of Appellate Procedure 4(b). The panel issued its opinion and judgment on August 24, 2021. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The First Amendment to the Constitution provides, in relevant part:

> Congress shall make no law . . . abridging the freedom of speech. . . .

The Fourth Amendment to the Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall

[3] Cert Appendix at 1a.

[4] Cert Appendix at 36a.

> issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Foreign Intelligence Surveillance Act ("FISA") is codified extensively at 50 U.S.C. §§ 1801 *et seq*. The provisions of FISA applicable to this Petition are included in the Appendix, at 52a-82a.

STATEMENT OF THE CASE

1. Surveillance Of Petitioner Based On The Federal Intelligence Surveillance Act

Based on the mandate of The Foreign Intelligence Surveillance Act ("FISA"), at 50 U.S.C. §§ 1801 *et seq*, neither the individual who is under surveillance pursuant to that statute nor his counsel, is ever permitted to know anything about what, how, when, why or for how long he was under surveillance. This applies to all levels of criminal trial and appellate litigation. Thus, the Petitioner, who was born in the United States and is a United States citizen, has no way of knowing anything about the extreme and personal government intrusion into his, and his family's lives.

Nonetheless, upon information and belief, in this matter, the Petitioner was subject to intrusive surveillance pursuant to FISA beginning in or around 2016, and continuing until he was taken into custody (August 23, 2018). Given that FISA only authorizes surveillance for at most a 90 day period of time (because the Petitioner is a United States citizen), the order authorizing the surveillance of the Petitioner was ostensibly extended multiple times. Each extension (re-application) would have required a separate finding of probable cause, and each finding of probable cause

allows a judge to consider past activities of a target, as well as "current or future activities" of the target. 50 U.S.C. § 1805(b).

The charges of which the Petitioner was found guilty were based wholly on evidence obtained from 243 electronically intercepted phone calls and 43 FaceTime sessions,[5] all of which were made accessible to the government solely by FISA surveillance. That surveillance was repeatedly authorized over a substantial period of time *before* the recorded communications indicated above were intercepted. Nonetheless, the Petitioner *was not, and to date still has not, been charged or indicted for any conduct which would justify the reduced Constitutional protections in legitimizing a FISA warrant that are authorized by that Act.*

2. <u>Indictment And Basis For Conviction</u>

On November 8, 2018, a Federal Grand Jury in the Eastern District of Virginia, Alexandria Division, returned an Indictment against the Petitioner. The Petitioner was charged with two counts of Coercion and Enticement of a Minor, in violation of 18 U.S.C. § 2422(b), and one count of Transfer of Obscene Materials to a Minor, in violation of 18 U.S.C. § 1470.

The first two counts relating to 18 U.S.C. § 2422(b) require the government to specify (an) underlying criminal offense(s) which address specific sexual activity. The government did that in this case. In Count 1, the underlying statutes were Title 18, United States Code, Section 2251, Code of Virginia, Section 18.2-374.1, and Minnesota Statutes, Section 617.246. In Count 2, the underlying statutes were Code

[5] JA 613.

of Virginia, Section 18.2-371, Code of the District of Columbia, Section 22-3008 and Code of Maryland, Criminal Law, Sections 3-307(a)(4) and (5).[6] Thus, *all of the alleged illegal conduct throughout this case was related solely to forms of sexual-related conduct.*

3. Petitioner's Motion To Suppress The Electronic Surveillance That Was Obtained Pursuant To FISA

A Motion to Suppress was filed by the Petitioner To Suppress Electronic Surveillance Obtained Without A Warrant And Without A Finding Of Probable Cause Of Criminal Conduct, And For Disclosure Of The FISA Applications To Defense Counsel.[7] As noted, the investigation of the Petitioner, and the evidence considered by the Judge during the trial in this matter was directly based on, and derived from 243 telephone conversations and 43 FaceTime sessions recorded by the Government. The authority upon which the Government relied to record the Petitioner's conversations was a FISA warrant.[8]

Upon information and belief, the government had obtained a FISA warrant against the Petitioner at least as far back as 2016. Also upon information and belief, authority for the surveillance of the Petitioner revealed no illegal activity until August 2018 *and revealed no terrorism or espionage related activities*, yet the FISA surveillance authority was apparently renewed every 90 days as required by law. 50 U.S.C. § 1805(d)(1). Nonetheless, in each application for FISA surveillance, the

---

[6] JA 111.1-111.4.

[7] JA 134.

[8] JA 5.

Government ostensibly continued to claim there was probable cause to believe that the Petitioner knowingly acted for or on behalf of a "foreign power" (as defined in FISA), or knowingly aided or abetted a "foreign power" (among other things).[9]

In the Motion to Suppress,[10] the Petitioner argued that all of the FISA evidence, (which directly led to all evidence presented in the case), should be suppressed because it was collected in violation of FISA, the First Amendment and the Fourth Amendment.[11] The motion was based on several grounds, including that the applications failed to establish a "reasonable, particularized ground for belief that the Petitioner qualified as an agent of a foreign power."[12] Also, that the FISA applications were predicated on protected First Amendment activities,[13] and/or that the underlying information used to satisfy the FISA probable cause standard was inaccurate, unreliable or contained intentional or reckless falsehoods or omissions.[14]

The Government filed a classified brief in opposition to the Petitioner's motion, along with the relevant FISA materials, all of which were submitted under seal and inaccessible to the Petitioner. The district court then undertook an *in camera*, *ex parte* review, and in a memorandum opinion, denied the motion.[15]

---

[9] JA 262-263.

[10] JA 134.

[11] JA 136.

[12] JA 140.

[13] JA 141, 143.

[14] JA 141-146.

[15] JA 254.

In denying the Motion to Suppress, the court first found that there was probable cause to believe that certain identified organization(s) were a "foreign power" and that "the target" (upon information and belief, Petitioner) knowingly acted for or on behalf of those organizations, or knowingly aided or abetted those organizations and was therefore an "agent(s) of a foreign power" under 50 U.S.C. §§ 1801(b)(2) and 1821(1).[16]

With regard to the First Amendment issue, without seemingly making a determination, the court stated "even if defendant were a/the target, it would have been permissible for the FISA application to refer to First Amendment-protected activities, provided that there was other evidence of prohibited activity."[17]

In its opinion, the court did not address any issues related to the underlying information used to satisfy the FISA probable cause standard, and failed to address why repeated renewals of the FISA authority in this case were appropriate, given that ostensibly there were no terrorist or espionage activities and thus the support for probable cause would have been diminished with each renewal.

4. <u>The Fourth Circuit's Opinion Failed To Address The Issue</u>

The Fourth Circuit Court of Appeals panel heard the same argument described above with regard to the suppression of the evidence obtained pursuant to FISA surveillance. The panel, like the district court below, failed to address the issues relating to probable cause and repeated renewals as described immediately above.

---

[16] JA 262.

[17] JA 263.

Instead, the *only* information expressed by the panel in support of its denial of the petition for appeal on this issue was "[h]aving reviewed the materials, and having fully considered Appellant's arguments, we affirm the district court's denial of Appellant's suppression motion."[18]

REASONS FOR GRANTING THE PETITION

THE ELECTRONIC SURVEILLANCE, AND EVIDENCE THEREFROM, OBTAINED BY THE GOVERNMENT PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT ("FISA"), WERE IN VIOLATION OF FISA AND/OR THE FIRST AND/OR FOURTH AMENDMENTS, AND SHOULD HAVE BEEN SUPPRESSED

I. BACKGROUND

Important differences exist between the standards for a FISA warrant and one issued under the Fourth Amendment or Title III of the U.S. Criminal Code. The "probable cause" required under FISA is merely that the target qualifies as an "agent of a foreign power," 50 U.S.C. § 1801(b), who will use the electronic device subject to electronic surveillance, or owns, possesses, uses, or is in the premises to be searched. *See* 50 U.S.C. §§ 1805(a)(3) & 1824(a)(3), and not that a crime has been, or is being, committed.

In considering an application for electronic surveillance pursuant to FISA, the Court should reject the application unless the application meets certain criteria sufficient to permit the Court to make the requisite findings under § 1805(a). For example, there must be probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . ." In addition, the

[18] Cert Appendix at 17a.

proposed minimization procedures must meet the definition of minimization procedures under § 1801(h), and the application must contain all required statements and certifications.

Also, in accordance with § 1805(a)(4), if a target is a "United States person," the FISC must determine whether the "certifications" under § 1804(a)(6)(E) – namely that the information sought is "the type of foreign intelligence information designated," and the information "cannot reasonably be obtained by normal investigative techniques" – are "not clearly erroneous." In addition, § 1805(a)(2)(A) provides "that no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment . . . ."

In this instance, it is undisputed that Mr. Kokayi is a United States citizen and that an order was entered to authorize a FISA warrant against Mr. Kokayi at some point in time. By statute, the duration of that surveillance was for "the period necessary to achieve its purpose, or for 90 days, whichever is less." 50 U.S.C. § 1805(d)(1). The requirement for issuing an order authorizing surveillance in this case is "on the basis of the facts submitted by the applicant there is probable cause to believe that … the target of the electronic surveillance is … an agent of a foreign power." 50 U.S.C. § 1805(a)(2)(A). A further requirement is that the facts submitted contain evidence of activities *not* protected by the first amendment to the Constitution of the United States. *Id*. The issuance of an order also requires a finding that "the proposed minimization procedures meet the definition of minimization procedures under [50 U.S.C.] section 1801(h)."

Upon information and belief, the order authorizing surveillance of Mr. Kokayi was extended multiple times. Each extension necessarily required new findings to be made, just as required for issuance of the original order. 50 U.S.C. § 1805(d)(2). That is, new probable cause must be found for each extension.

Moreover, "[i]n determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. § 1805(b).

Upon information and belief, the surveillance of Mr. Kokayi produced no evidence of terrorism related activities or clandestine intelligence gathering activities, as Mr. Kokayi was never charged with any terrorism or espionage related crimes.

II. ARGUMENT

A. FISA-Generated Evidence Should Have Been Suppressed Based On Likely Inappropriately Repeated and Extended Surveillance

Upon information and belief, the order authorizing surveillance of Mr. Kokayi was extended multiple times. Each extension necessarily required new findings to be made, just as required for issuance of the original order. 50 U.S.C. § 1805(d)(2). That is, new probable cause must be found for each extension.

Moreover, "[i]n determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. § 1805(b).

As noted, upon information and belief, the surveillance of Mr. Kokayi produced no evidence of terrorism related activities or clandestine intelligence gathering activities. Hence, each time that the surveillance order was renewed, the "past activities of the target" to be considered in determining probable cause incrementally contained longer and longer periods of time with no illegal terrorist or espionage related activities. This, in turn, should have diminished any probable cause finding with each extension. In addition, the current activities or the target to be considered in determining probable cause should also have contained no evidence of terrorist or espionage activities with each renewal.

B. FISA-Generated Evidence Should Have Been Suppressed Based On Additional Grounds

1. The FISA Applications May Have Failed to Establish the Requisite Probable Cause

Before authorizing FISA surveillance, the FISA Court must find, *inter alia*, probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power." § 1805(a)(2)(A). Under FISA, though, unlike with respect to a traditional warrant, the probable cause standard is directed *not* at the target's alleged commission of a crime, but at the target's alleged status as "a foreign power or an agent of a foreign power."

Consequently, the court must determine whether the application established a reasonable, particularized ground for belief that the defendant qualified as an agent of a foreign power. §§ 1805(a)(2)(A) & 1801(b)(2)(C) & (E). The court must also determine that such grounds continued to exist with each renewal.

In this case, absent an opportunity to review the applications for any of the surveillance at issue, defense counsel cannot specify whether the allegations asserting that the Petitioner was an "agent of a foreign power" were sufficient to satisfy FISA. Among FISA's definitions of "agent of a foreign power," § 1801(b)(2)(C) provides that the term includes: "any person . . . who *knowingly* engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." (Emphasis added).

If that provision was the basis for the FISA applications, the statute requires the presentation of evidence establishing probable cause that the Petitioner *knowingly* engaged in some type of international terrorism, and that the Petitioner *knew* that his activities were assisting "international terrorism."

In addition, because the Petitioner is a United States citizen, if the only activities relied upon by the government for the FISA warrant are protected speech under the First Amendment to the United States Constitution, the Petitioner cannot be considered a foreign power or an agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2)(A).

Accordingly, if the Petitioner participated in First Amendment activities such as expressing support, urging others to express support, gathering information, distributing information, raising money for political causes, or donating money for political causes, these activities cannot by themselves serve as a basis for probable cause for a FISA warrant. The statute reaches only material support coordinated with or under the direction of a designated foreign terrorist organization. *See Holder v.*

Humanitarian Law Project, 561 U.S. 1, 31-32 (2010) ("Independent advocacy that might be viewed as promoting the group's legitimacy is not covered.").

2. The FISA Applications May Have Contained Intentional or Reckless Falsehoods or Omissions In Contravention of *Franks v. Delaware*, 438 U.S. 154 (1978)

The Supreme Court's decision in *Franks v. Delaware*, 438 U.S. 154 (1978), established the circumstances under which the target of a search may obtain an evidentiary hearing concerning the veracity of the information set forth in a search warrant affidavit. As the Court in *Franks* instructed, "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statements necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Id.* at 156-57; *see United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (suggesting that *Franks* applies to FISA applications under Fourth and Fifth Amendments).

The *Franks* principles apply to omissions as well as to false statements. *See*, *e.g., United States v. Carpenter*, 360 F.3d 591, 596-97 (6th Cir. 2004); *United States v. Atkin*, 107 F.3d 1213, 1216-17 (6th Cir. 1997). Omissions will trigger suppression under *Franks* if they are deliberate or reckless, and if the search warrant affidavit, with omitted material added, would not have established probable cause. In this case, omissions would include withholding details concerning the lack of evidence obtained regarding terrorist or espionage activities during prior surveillance periods.

Without having had the opportunity to review the applications, the Petitioner was unable to point to or identify any specific false statements or material omissions in those applications. *See United States v. Daoud*, 755 F.3d 479, 493 (7th Cir. 2014) (Rovner, J., concurring) (explaining difficulty of reconciling *Franks* with denying access to FISA warrant applications, and concluding that "[w]ithout access to the FISA application, it is doubtful that a defendant could ever make a preliminary showing sufficient to trigger a *Franks* hearing.").

Although that lack of access prevented defense counsel from making the showing that *Franks* ordinarily requires, it is noted that the possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions is hardly speculative. For instance, in 2002, in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC), *rev'd on other grounds sub nom.*, *In re Sealed Case*, 310 F.3d 717 (FISCR, 2002),[19] the FISC reported that beginning in March 2000, the Department of Justice (hereinafter "DoJ") had come "forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts."

According to the FISC, "[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . ." *Id*. at 621. FISA-related overcollection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. *See* DoJ IG Report, at 29. The total percentage of FISA-

[19] "FISCR" refers to the Foreign Intelligence Court of Review.

related violations rose from 71% to 78% from 2004 to 2005, *id*. at 29, although the amount of time "over-collection" and "overruns" were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id*. at 25.

Thus, a *Franks* hearing, and disclosure of the underlying FISA materials, were necessary to permit the Appellant the opportunity to show that the affiants before the FISC intentionally or recklessly made materially false statements and/or omitted material information from the FISA applications.

3. The FISA Applications May Not Have Included Required Certifications

The Court should review the FISA applications to determine whether they contain all certifications required by § 1804(a)(6). As the Ninth Circuit has declared in the Title III context, "[t]he procedural steps provided in the Act require 'strict adherence,'" and "utmost scrutiny must be exercised to determine whether wiretap orders conform to [the statutory requirement]." *United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001), *quoting United States v. Kalustian*, 529 F.2d 585, 588-9 (9th Cir. 1975).

4. The FISA Applications, and the FISA Surveillance, May Not Have Contained or Implemented the Requisite Minimization Procedures

In order to obtain a valid FISA order, the government must include in its application a "statement of the proposed minimization procedures." § 1804(a)(4). The purpose of these minimization procedures is to (i) ensure that surveillance is reasonably designed to minimize the acquisition and retention of private information regarding people who are being wiretapped; (ii) prevent dissemination of non-foreign

intelligence information; and (iii) prevent the disclosure, use, or retention of information for longer than seventy-two hours unless a longer period is approved by Court order. § 1801(h).

FISA surveillance involves particularly intrusive electronic surveillance typically occurring on a continuous 24-hour basis, and *all* conversations are captured, with minimization occurring later and in other forms. Accordingly, minimization in the FISA context is critically important.

Here, the government provided an incredibly large amount of products of surveillance, including, without limitation, phone taps, listening devices in the Petitioner's home, and interception of electronic communication (including text message, Instagram messages, and emails). It is possible that the FISA application did not contain adequate minimization procedures or, if it did, that those procedures were not followed. In order to have determined whether there were adequate minimization procedures, and that the government complied therewith, defense counsel should have been provided with the FISA applications, orders, and related materials.

III. CONCLUSION

Based on the forgoing, the evidence obtained pursuant to the FISA warrant should have been suppressed.

Respectfully submitted,

/s/ Mark J. Petrovich
Mark J. Petrovich
Counsel of Record
PETROVICH & WALSH, PLC
10605 Judicial Drive, Suite A-5
Fairfax, Virginia 22030
(703) 934-9191
mp@pw-lawfirm.com

Anthony H. Nourse
LAW OFFICE OF ANTHONY H. NOURSE, PLC
4151 Chain Bridge Road
Fairfax, Virginia 22030
(703) 881-9161
ahn@fairfaxdefense.com