No. 14-_____

In the Supreme Court of the United States

ADEL DAOUD,

Petitioner,

–v–

UNITED STATES OF AMERICA,

Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Seventh Circuit

PETITION FOR WRIT OF CERTIORARI

JOHN D. CLINE
235 MONTGOMERY STREET,
SUITE 1070
SAN FRANCISCO, CA 94104

MATTHEW R. SEGAL
JESSIE J. ROSSMAN
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
MASSACHUSETTS
211 CONGRESS STREET,
3RD FLOOR
BOSTON, MA 02110

HARVEY GROSSMAN
ROGER BALDWIN
FOUNDATION OF ACLU, INC.
180 N. MICHIGAN AVENUE,
SUITE 2300
CHICAGO, IL 60601

THOMAS ANTHONY DURKIN
COUNSEL OF RECORD
JANIS D. ROBERTS
JOSHUA G. HERMAN
DURKIN & ROBERTS
2446 NORTH CLARK STREET
CHICAGO, IL 60614
(312) 913-9300
TDURKIN@DURKINROBERTS.COM

JAMEEL JAFFER
STEVEN R. SHAPIRO
PATRICK TOOMEY
ASHLEY M. GORSKI
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 BROAD STREET
NEW YORK, NY 10004

DECEMBER 31, 2014 *COUNSEL FOR PETITIONER*

SUPREME COURT PRESS ♦ (888) 958-5705 ♦ BOSTON, MASSACHUSETTS

QUESTION PRESENTED

The Foreign Intelligence Surveillance Act of 1978 ("FISA") authorizes courts to order disclosure, under appropriate security procedures, of FISA surveillance applications and orders to criminal defendants whom the government has subjected to surveillance under the statute. 50 U.S.C. §§ 1806(f), 1825(g). If the Attorney General files an affidavit stating that disclosure of the FISA materials would harm national security, the court may order disclosure "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.*

The effect of the Seventh Circuit's construction of Section 1806(f) was to deny disclosure of FISA materials even in those cases where, as here, the surveillance raises unusually complex questions of fact and law, and where the district court concludes, after an initial *ex parte* review of the relevant materials, that limited disclosure to defense counsel would meaningfully enhance the court's ability to make an accurate determination of the legality of the surveillance.

The question presented is:

Whether the Seventh Circuit's construction of Section 1806(f) is consistent with this Court's decision in *Franks v. Delaware*, 438 U.S. 154 (1978), and with the Fourth and Fifth Amendments?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES—Continued

Page

TABLE OF AUTHORITIES—Continued

CONSTITUTIONAL PROVISIONS

FEDERAL STATUTES

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

PETITION FOR WRIT OF CERTIORARI

Petitioner Adel Daoud respectfully submits this petition for a writ of certiorari.

OPINIONS BELOW

The opinions of the Seventh Circuit Court of Appeals are reported at 755 F.3d 479 and 761 F.3d 678 and reprinted in the Appendix at 14a–51a and 1a–13a. The opinion of the District Court for the Northern District of Illinois is not published but is available at 2014 WL 321384 and reprinted in the Appendix at 52a–58a.

JURISDICTION

The judgment of the court of appeals was entered on June 16, 2014. On July 24, 2014, the court of appeals extended the time within which to file a petition for rehearing en banc to and including August 12, 2014. A timely petition for rehearing en banc was denied on October 2, 2014. Pet. App. 59a. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The following constitutional and statutory provisions are set forth in the Appendix at 60a:

- U.S. Const. amend. IV
- U.S. Const. amend. V
- 50 U.S.C. § 1806

INTRODUCTION

This case raises a recurring question of national importance: When is a criminal defendant who is being prosecuted based on evidence acquired under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, entitled to examine applications, orders, and other materials relating to that surveillance? Since FISA was enacted in 1978, courts have struggled to reconcile 50 U.S.C. § 1806, which permits disclosure of FISA materials in only limited circumstances, with the Fourth and Fifth Amendments, which guarantee criminal defendants a meaningful opportunity to seek the suppression of evidence that was obtained unlawfully.[1] They have

[1] Throughout this Petition, in an effort to avoid duplication, Petitioner focuses principally on Section 1806(f), which governs disclosure of FISA materials relating to electronic surveillance, rather than on Section 1825(g), which governs disclosure of FISA materials relating to physical surveillance. The relevant

struggled in particular to reconcile the language of Section 1806(f) with *Franks v. Delaware*, in which this Court held that criminal defendants are entitled to an evidentiary hearing upon a "substantial preliminary showing" that a warrant affidavit includes a knowing or reckless false statement. 438 U.S. 154, 155–56 (1978). Section 1806(f) plainly contemplates that FISA materials will be disclosed to defendants in some circumstances, and many courts construing Section 1806(f) have acknowledged, as the concurrence did below, that a narrow reading of the statute is difficult to reconcile with the Fourth and Fifth Amendments. Until this case, however, no district court had ordered the government to disclose FISA materials to any defendant—and in this case, the Seventh Circuit reversed the district court's decision.

The question of when defendants are entitled to see FISA materials is a recurring one because the use of FISA-derived evidence in national-security prosecutions is now routine.[2] The question takes on

---

portions of the two provisions are almost identical, however, and Petitioner's arguments apply to the two provisions equally.

[2] Throughout this petition, Petitioner uses the phrase "disclosure to defendants" as a shorthand for disclosure under the conditions contemplated by Sections 1806(f) and 1825(g), but it is important to note that those provisions contemplate disclosure under "appropriate security procedures and protective orders," or by having the Attorney General provide "summar[ies]" of the relevant materials. 50 U.S.C. §§ 1806(f), 1825(g). For example, a protective order may require that disclosure of FISA materials be limited to security-cleared defense counsel who can access the materials only in a Sensitive Compartmented Information Facility. *See also* Classified Information Procedures Act, 18 U.S.C. App. 3 § 4.

even more importance, however, in light of the vast expansion of the government's surveillance activities since 2001; the government's aggressive use of new surveillance authorities whose constitutionality is deeply contested; the government's reliance on the fruits of surveillance conducted under those authorities to secure FISA orders; and uncertainty about when the government is obliged to notify defendants that any of these authorities were used against them. Denied access to applications, orders, and other materials relating to the government's surveillance, criminal defendants are unable to determine precisely which surveillance authorities were used against them, or in what ways they were used, let alone establish the factual predicate that would entitle them to *Franks* hearings. Denied access to these materials, it is difficult or impossible for many defendants to exercise rights guaranteed by the Fourth and Fifth Amendments.

That criminal defendants cannot meaningfully exercise these rights also creates a deeper structural problem—one that implicates the rights of nearly all Americans. Outside the context of criminal prosecutions, the government does not ordinarily notify those whose communications it has monitored under FISA, the FAA, or other national-security authorities. As a result, those whose privacy is implicated by surveillance conducted under these authorities generally lack the ability to contest the constitutionality of the authorities or the government's use of them. Motions to suppress in criminal prosecutions are the principal means, and in many contexts the *only* means, by which the constitutionality of government surveillance

conducted for national-security purposes can be tested. To the extent that criminal defendants are denied access to the materials that would allow them to challenge the lawfulness of this surveillance, the surveillance is shielded from judicial review and effectively placed beyond the reach of the Constitution.

An unduly narrow construction of Section 1806(f) infringes the Fourth and Fifth Amendments and inappropriately insulates far-reaching surveillance activities from judicial review. Section 1806(f) must be construed to require disclosure in at least those cases where, as here, the surveillance raises unusually complex questions of fact and law, and where the district court has concluded, after an *ex parte* review of the relevant materials, that limited disclosure to defense counsel would meaningfully enhance its ability to make an accurate determination of the legality of the surveillance.

This Court should grant certiorari to clarify the meaning of Section 1806(f).

STATEMENT OF THE CASE

1. In 1978, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny government applications for surveillance orders in certain foreign intelligence investigations. *See* 50 U.S.C. §§ 1803(a),

1804–1805 (electronic surveillance); *see also id.* §§ 1822–1825 (physical searches). In its current form, FISA prohibits the government from engaging in certain types of "electronic surveillance," *id.* § 1801(f), without first obtaining an individualized order from the FISC. To obtain an order, the government's application must identify or describe the target of the surveillance; explain the government's basis for believing that "the target of the electronic surveillance is a foreign power or an agent of a foreign power"; explain the government's basis for believing that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power"; describe the procedures the government will use to minimize the acquisition, retention, and dissemination of information concerning U.S. persons;[3] describe the nature of the foreign intelligence information sought and the type of communications that will be subject to surveillance; and certify that a "significant purpose" of the surveillance is to obtain "foreign intelligence information." *Id.* § 1804(a). The FISC can issue an order authorizing surveillance only if it finds, *inter alia*, that there is "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power," *id.* § 1805(a)(2)(A); and that "each of the facilities or places at which the electronic surveillance is directed

---

[3] FISA defines "U.S. person" to include U.S. citizens, aliens lawfully admitted for permanent residence, and certain corporations and unincorporated associations. 50 U.S.C. § 1801(i).

is being used, or is about to be used, by a foreign power or an agent of a foreign power," *id.* § 1805(a)(2)(B).

In 2008, Congress enacted the FISA Amendments Act ("FAA"), which substantially revised the FISA regime by allowing for the large-scale interception of U.S. persons' international communications without probable cause or individualized judicial approval of the government's surveillance targets. *See* 50 U.S.C. § 1881a; *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). While as a general matter the government must still obtain individualized FISA orders if it intends to "target" U.S. persons for surveillance, the FAA permits the government to collect U.S. persons' communications without individualized suspicion in the course of surveillance directed at foreigners abroad. Surveillance conducted pursuant to the FAA raises significant and complex constitutional questions that have not yet been considered by any appellate court.

Ordinarily, persons whose communications are monitored under FISA and the FAA do not receive notice of the government's surveillance. However, where the government intends to rely on evidence "obtained or derived" from FISA or the FAA in a criminal prosecution, notice to the defendant is statutorily required. 50 U.S.C. §§ 1806(c), 1825(d), 1881e. A defendant who is notified of FISA or FAA surveillance may move for disclosure of applications, orders, and other materials related to the surveillance, and for suppression of the resulting evidence. *See id.* §§ 1806(e), 1825(f). If the defendant moves for disclosure, the Attorney General must

determine whether to file an affidavit asserting that disclosure or an adversary hearing would harm the national security of the United States. *See id.* §§ 1806(f), 1825(g). If the Attorney General files such an affidavit, the statute directs the district court to review materials relating to the surveillance *in camera* and *ex parte* "as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.* § 1806(f).

The statute recognizes, however, that in some cases the district court's *in camera* and *ex parte* review will not be sufficient or conclusive and that an adversarial process will be necessary. Thus, the statute provides that, following the court's initial review, the court may disclose FISA materials to the defendant under appropriate security procedures and protective orders "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.*

Although the statute plainly contemplates disclosure of FISA materials in some cases, since 1978 the Attorney General has filed an affidavit opposing disclosure in every case in which a defendant has sought disclosure. Until this case, no court had ever ordered the government to disclose FISA materials to a criminal defendant.

2. On September 15, 2012, after an FBI "sting" operation, the government filed a criminal complaint charging Petitioner, an 18-year-old American citizen and resident of Hillside, Illinois, with attempting to use a weapon of mass destruction and attempting to damage and destroy a building by means of an

explosive. Three days later, the government notified Petitioner, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), that it intended to present evidence at his trial "obtained and derived" from surveillance conducted under FISA.

Although the government's notice mentioned only FISA, and not the FAA, questions arose shortly thereafter about the government's reliance on the FAA in Petitioner's case. Most significantly, on December 27, 2012, Senator Dianne Feinstein, who was then the Chairman of the U.S. Senate Select Committee on Intelligence, stated in a debate concerning the reauthorization of the FAA that Petitioner's case was among those that showed the necessity and effectiveness of the statute. *See* 158 Cong. Rec. S8393 (daily ed. Dec. 27, 2012) (statement of Sen. Dianne Feinstein) (listing a series of terrorism-related cases, including Petitioner's case, and then remarking that "the FISA Amendments Act is important and these cases show the program has worked").[4]

Other disclosures have underscored the possibility that the FAA might have been used in Petitioner's case. For example, the Privacy and Civil

---

[4] Counsel for the Senate Intelligence Committee later wrote that Senator Feinstein had not meant to imply that the FAA had (or had not) actually been used against Petitioner. *See* Letter from Morgan J. Frankel, Counsel, United States Senate Select Committee on Intelligence, to Thomas Anthony Durkin (Sept. 16, 2013) ("[N]othing in Senator Feinstein's remarks was intended to convey any view that FAA authorities were used or were not used in Mr. Daoud's case or in any of the other cases specifically named.").

Liberties Oversight Board ("PCLOB") reported that the FBI searches its database of FAA-obtained information "whenever the FBI opens a new national security investigation or assessment."[5]

The Department of Justice informed Petitioner that it "does not intend to use any such evidence obtained or derived from FAA-authorized surveillance in the course of this prosecution." Gov't Sur-Reply to Def. Mot. for Notice of FAA Evidence at 2, *United States v. Daoud*, No. 12-cr-723 (N.D. Ill. Aug. 8, 2013), ECF No. 49. It declined to say, however, whether the FAA was used to collect or monitor Petitioner's communications, and it has not disclosed the meaning it accords to the phrase "obtained or derived"—though, as discussed below, *see* Section I, *infra*, the government has conceded that it interpreted that phrase too narrowly in the past.

3. On August 9, 2013, Petitioner moved for disclosure of FISA materials to his security-cleared

---

[5] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ("PCLOB Report"), at 59.

Later, at an *ex parte* hearing, the Seventh Circuit repeatedly asked the government whether it had relied on the FAA in its surveillance of Petitioner. The government's responses are redacted from the publicly available transcript. *See* Pet. App. 68a–69a, 71a–73a, 74a–76a. Following that *ex parte* hearing, the court specifically asked the government whether the FAA had played "any role, no matter how minimal," in the investigation of Petitioner. *See* Pet. App. 11a. The government apparently addressed the question at some length, but the court redacted the government's answer from the public version of its classified opinion. *See id.*

defense counsel pursuant to Section 1806(f); requested a *Franks* hearing; and sought to suppress all evidence obtained or derived from surveillance under FISA. Because Petitioner lacked access to the underlying FISA materials, his argument as to the unlawfulness of the FISA surveillance was to some degree speculative. Based on the limited information available to him, however, Petitioner identified several potential theories under which some of the evidence against him should be suppressed. One of these theories was that the FISA applications included knowing or reckless falsehoods. Another was that information the government submitted in support of its FISA applications was the product of unlawful surveillance conducted under the FAA. *See* Def. Mem. in Support of Mot. for Disclosure of FISA-Related Material at 15, *United States v. Daoud*, No. 12-cr-723 (N.D. Ill. Aug. 9, 2013), ECF No. 52.

In response, the Attorney General filed an affidavit stating that national security would be harmed by disclosure of the FISA materials to Petitioner's security-cleared counsel. This filing triggered an *in camera*, *ex parte* review by the district court to determine whether disclosure of the materials was necessary to make an accurate determination of the legality of the surveillance. *See* 50 U.S.C. §§ 1806(f), 1825(g).

After conducting a "thorough and careful review" of the FISA materials, the district court granted Petitioner's motion in part, ordering the disclosure of the FISA application materials to his security-cleared counsel, subject to a protective order. Pet. App. 57a. The district court stated that its decision

was "not made lightly," but that it had concluded that "disclosure may be necessary." *Id.* While the court acknowledged that it was "capable" of deciding the legality of the surveillance without adversarial process, it reasoned that "an accurate determination of the legality of the surveillance [would be] best made in this case as part of an adversarial proceeding." *Id.*[6]

4. On appeal, the Seventh Circuit held that the district court had misconstrued Section 1806(f) and had ordered disclosure of FISA materials in circumstances in which the statute prohibited it. The court of appeals reasoned that disclosure of FISA materials could not have been "necessary" within the meaning of the statute if the district court was "capable" of adjudicating the lawfulness of the surveillance without disclosure, as the district court said it was. Pet. App. 19a, 25a. The Seventh Circuit also found significant that the district court had concluded only that disclosure "*may be* necessary," a conclusion that, in the Seventh Circuit's view, was insufficient to satisfy the statutory standard for disclosure. *Id.* at 19a (emphasis added).

Based on its own review of the FISA materials, and following an *ex parte* hearing with the government, the Seventh Circuit concluded that disclosure was unnecessary and that the surveillance and searches at issue were lawful. *See id.* at 25a–27a, 67a.

---

[6] In addition to ordering disclosure, the district court denied Petitioner's motion to suppress without prejudice. *Id.*

Judge Posner's opinion for the court acknowledged that denying a defendant access to FISA materials would make it "difficult[]" for a defendant to establish his entitlement to a *Franks* hearing. *Id.* at 23a ("Defense counsel would like to mount [a *Franks*] challenge in this case. But that's hard to do without access to the classified materials on which the government relied in obtaining a warrant. . . . "). The opinion concluded, however, that FISA reflected the view that "[c]onventional adversary procedure . . . [had] to be compromised in recognition of valid social interests that compete with the social interest in openness," *id.* at 22a, and that the district court had erred in ordering the government to disclose materials to security-cleared defense counsel, *id.* at 25a–27a.

Judge Rovner concurred in the result but wrote separately to address the difficulty of reconciling Section 1806(f) with *Franks*. Judge Rovner explained that, "[a]s a practical matter, the secrecy shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks*." Pet. App. 29a. Without access to the FISA application, she observed, "it is doubtful that a defendant could ever make a preliminary showing sufficient to trigger a *Franks* hearing," because "a defendant cannot identify such misrepresentations or omissions, let alone establish that they were intentionally or recklessly made." *Id.* at 46a, 29a. Judge Rovner underscored that "*Franks* serves as an indispensable check on potential abuses of the warrant process," and urged that "means must be found to keep *Franks* from becoming a dead letter in the FISA context." *Id.* at 30a.

In a separate classified opinion, much of which is redacted, the court of appeals explained why its study of the materials led it to believe that the government's surveillance of Petitioner under FISA was not unlawful. Pet. App. 1a–2a. The court concluded that, because the FISA surveillance was legal, "a remand to the district court is neither necessary nor appropriate," and "the information collected from the resulting surveillance should . . . not be suppressed." *Id.* at 2a, 13a.

On August 12, 2014, Petitioner timely petitioned for rehearing en banc. The petition was denied on October 2, 2014. Pet. App. 59a.

REASONS FOR GRANTING THE PETITION

I. THE QUESTION OF WHEN A CRIMINAL DEFENDANT IS ENTITLED TO REVIEW APPLICATIONS, ORDERS, AND OTHER MATERIALS RELATING TO FISA SURVEILLANCE IS A RECURRING QUESTION OF NATIONAL IMPORTANCE

1. The question of when a criminal defendant is entitled to review FISA materials is a recurring one. This is in part because the government relies on FISA much more often today than it did when FISA was first enacted.[7] When FISA-derived evidence is

[7] Whereas in 1978 the government obtained 207 electronic surveillance orders under FISA, in 2013 it obtained 1588. *See* Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, U.S. Dep't of Justice, to The Hon. Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2014), *available at*

used in criminal prosecutions, defendants routinely move under Section 1806(f) for access to applications, orders, and other materials relating to the surveillance, and the government routinely opposes such access. As a result, the question of whether a defendant should be afforded access to FISA materials is one that arises frequently.

The question is an important one for criminal defendants, because without access to FISA materials, it is virtually impossible for defendants to challenge the lawfulness of the government's surveillance of them. One example is the difficulty a defendant faces in establishing his right to a *Franks* hearing. In *Franks,* this Court held that a defendant is entitled to a hearing where he can make a "substantial preliminary showing" that a search warrant affidavit included a knowing or reckless false statement by the affiant. *Franks*, 438 U.S. at 155–56. But defendants cannot identify knowing or reckless falsehoods in affidavits they have not seen. As Judge Rovner observed in concurrence below, *see* Pet. App. 29a, 46a–47a, and as many other courts have similarly observed, *see* Section II, *infra*, defendants' lack of access to FISA materials makes it nearly impossible for them to exercise the rights recognized in *Franks*.

In addition, without access to FISA materials, it is difficult or impossible for defendants to determine which surveillance authorities were used against

---

http://www.fas.org/irp/agency/doj/fisa/2013rept.pdf; Letter from Benjamin R. Civiletti, Attorney General, U.S. Dep't of Justice, to The Vice President (1979), *available at* http://www.fas.org/irp/agency/doj/fisa/1979rept.html.

them—which means that they cannot effectively contest the legality of those authorities or the admissibility of evidence obtained through the use of those authorities. While the government is required to notify criminal defendants when it intends to rely on evidence "obtained or derived" from FISA, the government does not ordinarily notify defendants of the surveillance authorities that it used to obtain the evidence cited in its FISA applications. For example, it does not notify defendants when its FISA applications were based on evidence obtained using Executive Order 12,333, *see Clapper*, 133 S. Ct. at 1149; the "national-security letter" authorities, *see* 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u–1681v; 18 U.S.C. § 2709; or FISA's "business records" authority, *see* 50 U.S.C. § 1861—the provision the government is using to collect the phone records of millions of Americans, *see* PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court* (Jan. 23, 2014), at 115.

While the government *is* statutorily required to notify criminal defendants when it intends to rely on evidence obtained or derived from the FAA, *see* 50 U.S.C. §§ 1881e(a), 1806(c), in practice the government has read the phrase "obtained or derived" narrowly to deny notice to defendants whom the government now acknowledges should have received it. In its briefing and at oral argument before this Court in *Clapper*, the government represented that criminal defendants who were being prosecuted based on evidence obtained or derived from the FAA would receive notice of such

surveillance, and that those defendants would be able to challenge the constitutionality of the FAA. *See* Pet. Br. at 8, *Clapper*, 133 S. Ct. 1138 (July 26, 2012); Tr. 2–4, *id.* (Oct. 29, 2012). When this Court held that the plaintiffs in *Clapper* lacked standing to pursue their civil challenge to the statute, the Court accepted the government's representations as evidence that the dismissal of plaintiffs' challenge would not insulate the statute from judicial review. *See Clapper*, 133 S. Ct. at 1154. Several months after the Court issued its decision in *Clapper*, however, it became evident that the government had been construing its notice obligations too narrowly and that defendants who were entitled to notice had not received it. (In fact, the government did not provide an FAA notice to *any* defendant between 2008 and late 2013.) Only after some defendants filed motions seeking to enforce the FAA's notice provision did the government reconsider its notice policy. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, http://nyti.ms/1sBRGDr. Beginning in October 2013, the government began providing FAA notices to defendants who should have received those notices several years earlier.

The difficulty for defendants in overcoming their lack of access to FISA materials is compounded because the scope and complexity of the government's surveillance activities have increased dramatically since FISA was enacted. National-security surveillance now includes new forms of electronic eavesdropping, such as the interception of email and internet communications, as well as wide-ranging searches of electronic devices and stored

media. Given the scope and complexity of these activities, it is not generally possible for a defendant to overcome his lack of access to FISA materials simply by speculating about the surveillance authorities that might have been used against him. Even if a defendant managed to guess which surveillance authorities were used to obtain the evidence on which the government's FISA applications were predicated, the defendant's ability to challenge the lawfulness of the surveillance would be hobbled by his lack of knowledge about how those authorities were actually used.

2. Petitioner's case highlights these problems. The government has informed Petitioner that it intends to use evidence "obtained and derived" from FISA. It has not explained, however, what surveillance authorities were used to obtain the evidence on which its FISA applications and orders were predicated. Evidence in the public domain strongly suggests that the government used the FAA to obtain Petitioner's communications, *see* pp. 9–10 & nn.4–5, *supra*, but the government has not provided Petitioner with an FAA notice. In theory, Petitioner could file a motion consisting of hypothetical arguments (e.g., "If the government used FAA-derived evidence to obtain its FISA warrants, the FISA-derived evidence should be suppressed as the fruit of the poisonous tree because the FAA is unconstitutional on its face."), but Petitioner's argument would of necessity be abstract, and his ability to make an effective argument would be severely compromised by his lack of knowledge about whether or how the FAA was actually used against him.

Which of Petitioner's communications were acquired by the government under the FAA, and when? Was the government's surveillance target a legitimate one? Were Petitioner's communications obtained "incidentally" or "inadvertently"? What role did those communications play in the government's FISA application? Were they obtained directly from U.S. technology companies or were they acquired through the government's access to telecommunications infrastructure? Did the government comply with statutorily-required minimization procedures? Were those minimization procedures constitutional? Without access to the underlying FISA materials, Petitioner cannot know the answer to any of these questions—but without answers to these questions, Petitioner cannot meaningfully exercise the rights that the Fourth and Fifth Amendments guarantee.

3. This is a problem for Petitioner, but it is a structural problem, too. Some of the government's national-security surveillance activities are far-reaching and involve the collection of communications belonging to hundreds of millions of Americans. Because the government does not ordinarily notify those whose communications it has monitored, those whose privacy is implicated generally lack the ability to contest the constitutionality of the authorities or the government's use of them. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147–53 (2013) (plaintiffs who could not show high likelihood that FAA had been used to intercept their communications lacked standing to challenge statute's constitutionality); *ACLU v. NSA*, 493 F.3d 644, 648 (6th Cir. 2007)

(plaintiffs who could not show with certainty that their communications had been intercepted under warrantless wiretapping program lacked standing to challenge program's constitutionality).

Against this background, motions to suppress in criminal prosecutions are the principal means, and in many contexts the *only* means, by which the constitutionality of government surveillance conducted for national-security purposes can be tested. *Cf. Clapper*, 133 S. Ct. at 1154. To the extent that criminal defendants are denied access to the materials that would allow them to challenge the lawfulness of government surveillance, this surveillance is shielded from judicial review and, as a practical matter, placed beyond the reach of the Constitution.

II. THE SEVENTH CIRCUIT'S CONSTRUCTION OF SECTION 1806 CONFLICTS WITH *FRANKS* AND WITH DEFENDANTS' CONSTITUTIONAL RIGHT TO SEEK SUPPRESSION OF ILLEGALLY OBTAINED EVIDENCE

1. Together, the Fourth and Fifth Amendments require that defendants be afforded a meaningful opportunity to seek suppression of evidence that was obtained illegally.[8]

As this Court has made clear, "the Constitution requires the exclusion of evidence obtained by certain violations of the Fourth Amendment." *Sanchez-Llamas v. Oregon*, 548 U.S. 331, 348 (2006); *see also*

---

[8] FISA itself also requires the suppression of evidence obtained or derived from unlawful surveillance. *See* 50 U.S.C. §§ 1806(g), 1825(h).

Wong Sun v. United States, 371 U.S. 471, 486–88 (1963) (describing "fruit of the poisonous tree" doctrine); *Murray v. United States*, 487 U.S. 533, 536–38 (1988) (describing right to seek suppression of evidence "derived" from an unlawful search). In addition, in *Franks* the Court held that a search warrant must be voided, and the fruits of the search excluded, when a defendant proves by a preponderance of the evidence that the affidavit on which a warrant was based contained false statements that were either deliberately or recklessly made; and the court determines that the remainder of the affidavit was insufficient by itself to establish probable cause. 438 U.S. at 155–56. In the same case, the Court also held that the Fourth Amendment requires an evidentiary hearing where a defendant makes a "substantial preliminary showing" that a search warrant was the product of an intentionally or recklessly false or misleading affidavit. *Id.* at 155; *see also Alderman v. United States*, 394 U.S. 165, 180–84 (1969).

Under the Fifth Amendment's Due Process Clause, defendants must be afforded a process that permits them to seek the suppression remedy. *See, e.g., United States v. Phillips*, 540 F.2d 319, 325–26 (8th Cir. 1976) (party seeking to suppress fruit of unlawful surveillance must be given a "full and fair opportunity" to meet prima facie burden of showing that the surveillance was unlawful). While this Court has said that the interests at stake in a suppression hearing are of a "lesser magnitude" than those at stake in a criminal trial, it has concluded that Fifth Amendment due process protections apply in the pre-trial suppression context. *United States v. Raddatz*,

447 U.S. 667, 679 (1980). Consistent with this conclusion, circuit courts have held that the government must disclose information to a defendant that could affect the outcome of a suppression hearing. *See, e.g.*, *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different."); *Smith v. Black*, 904 F.2d 950, 965–66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992) (due process mandates the disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression hearing").

2. Section 1806 must be construed against this constitutional background. In particular, the statute must be construed to require disclosure of FISA materials in at least those cases where, as here, the surveillance raises unusually complex questions of fact and law, and where the district court concludes, after an initial *ex parte* review of the relevant materials, that limited disclosure to defense counsel would meaningfully enhance the court's ability to make an accurate determination of the legality of the surveillance. In at least this category of cases, disclosure of FISA materials under appropriate security measures is "necessary" for "an accurate determination of the legality of the surveillance," 50 U.S.C. § 1806(f), and it is also necessary as a matter of constitutional right.

As a general matter, adversarial proceedings are likely to enhance district courts' ability to make "accurate determination[s] of the legality of . . . surveillance." *Id.* Information that is seemingly inconsequential to a judge in an *ex parte* setting—"a chance remark, a reference to what appears to be a neutral person or event . . . or even the manner of speaking"—may have "special significance" to those who know the more intimate facts of a defendant's life. *Alderman v. United States*, 394 U.S. 165, 182 (1969); *see also* Pet. App. 47a. As Justice Frankfurter observed, "fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and [an] opportunity to meet it." *Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 170–72 (1951) (Frankfurter, J., concurring); *Franks*, 438 U.S. at 155, 169 (noting that a magistrate judge "has no acquaintance with the information that may contradict" the affidavit and rejecting the argument that *ex parte* review by a magistrate judge would sufficiently protect defendants' rights).

Likewise, adversarial process substantially improves the quality and fairness of the legal arguments considered by a reviewing court. A court that hears from only the government may overlook key legal arguments that would be raised by defense counsel, such as those directed at the nature and scope of the government's electronic searches, which are often governed by a patchwork of legal authorities and new precedents.

Importantly, the *ex parte* process that suffices when a search warrant is issued is not necessarily adequate once a defendant's liberty is at stake. The availability of adversarial process provides a crucial layer of protection against government error and overreaching when the government's interest has shifted from foreign-intelligence investigation to prosecution. This added layer of protection is necessary because once a prosecution is initiated, the citizen's interest is substantially higher. The consequence of error is no longer limited to an unwarranted invasion of the target's privacy, as it is when the FISC initially reviews the government's *ex parte* surveillance application. Rather, defendants in national-security cases typically face severe criminal penalties, and "the resolution of a suppression motion can and often does determine the outcome of the case." *Raddatz*, 447 U.S. at 677–78. Meaningful participation by defense counsel at the suppression stage ensures that the district court's review is not a mere repetition of the FISC's *ex parte* process, where that court is entirely reliant on the government's representations and is insulated from informed counterarguments.

Adversarial process is almost always preferable, but it is especially necessary where factual or legal issues are unusually complex. As this Court has explained:

> [T]he need for adversary inquiry is increased by the complexity of the issues presented for adjudication. . . . Adversary proceedings will not magically eliminate all error, but they will substantially reduce its

> incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands.

Alderman, 394 U.S. at 182, 184; *cf. Taglianetti v. United States*, 394 U.S. 316, 317 (1969) (per curiam) (suggesting that, where a court's task is "'too complex, and the margin for error too great,'" *ex parte* proceedings would be "an inadequate means to safeguard a defendant's Fourth Amendment rights" (quoting *Alderman*, 394 U.S. at 182)).

A traditional due process analysis underscores that adversarial process is necessary at least where factual or legal issues are particularly complex. Under *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976), three factors to be considered in evaluating the sufficiency of procedural protections are: (1) "the private interest that will be affected by the official action"; (2) "the risk of an erroneous deprivation of such interest through the procedures used, and the probative value, if any, of additional or substitute procedural safeguards"; and (3) "the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail."

All three of these factors weigh in favor of requiring disclosure of FISA materials in the category of cases described above. First, defendants have a substantial interest in an accurate determination of whether the government's

surveillance violated their rights, and thus whether the fruits of that surveillance may be suppressed. *See Raddatz*, 447 U.S. at 677–78. Second, where factual or legal issues are particularly complex, a district court's *in camera* and *ex parte* review of the materials carries an unacceptably high risk of error. *Cf. United States v. James Daniel Good Real Prop.*, 510 U.S. 43, 55 (1993) ("The practice of *ex parte* seizure . . . creates an unacceptable risk of error."); *Alderman*, 394 U.S. at 180–84. Finally, the government's interest in secrecy in this context, while not insignificant, can be accommodated through "appropriate security procedures and protective orders" or by having the Attorney General provide "summar[ies]" of the relevant materials. 50 U.S.C. §§ 1806(f), 1825(g); *see also* Classified Information Procedures Act, 18 U.S.C. App. 3.

Indeed, it bears emphasis that disclosure in this context does not necessarily mean disclosure to all, or disclosure of everything. Both the statute and the Constitution permit—indeed, require—a more nuanced approach. *See* 50 U.S.C. §§ 1806(f), 1825(g). The mere fact that the government has a legitimate interest in withholding some FISA information does not mean it has a legitimate interest in withholding all of it; and the mere fact that the government has a legitimate in interest in withholding FISA information from the general public (or even from the defendant) does not mean that it has a legitimate interest in withholding it from defense counsel,

particularly if that defense counsel has security clearance.[9]

Accordingly, the Fourth and Fifth Amendments counsel in favor of construing Section 1806 to require disclosure of FISA materials where the relevant factual or legal questions are particularly complex, and where the court itself concludes that adversarial process would enhance its ability to make an accurate determination of the legality of the surveillance.

3. The Seventh Circuit construed Section 1806 too narrowly. Following many other courts, the Seventh Circuit construed the statute in a manner that forecloses disclosure of FISA materials even where doing so deprives a defendant of any meaningful opportunity to seek suppression of evidence that was obtained illegally. Since FISA was enacted in 1978, no defendant has been able to access FISA materials under Section 1806, even though the statute plainly contemplates that FISA materials should sometimes be disclosed. The prevailing reading of Section 1806 is in deep tension with the Fourth and Fifth Amendments—and, unusually,

---

[9] Outside of the FISA context, when the government asserts a privilege that conflicts with a criminal defendant's right to seek suppression, courts carefully balance a defendant's due process rights against the government's assertion of the privilege. *See, e.g.*, *United States v. Green*, 670 F.2d 1148, 1155–56 (D.C. Cir. 1981) (government interest in protecting police surveillance locations from disclosure must be balanced against a defendant's "strong interest in effective cross-examination of adverse witnesses at a suppression hearing").

many of the courts that have adopted this construction have conceded as much.

The Seventh Circuit's error was in concluding that Section 1806 barred disclosure of FISA materials even though the case involved factual and legal questions that were particularly complex, and even though the district court had concluded that disclosure of FISA materials to security-cleared counsel would enhance the court's ability to make an accurate determination of the legality of the surveillance. Petitioner's case is particularly complex, not least because information in the public record suggests that the FAA may have played some as-yet undisclosed role in the government's investigation. *See* pp. 9–10 & nn.4–5, *supra*. Whether the FISC's order authorizing FISA surveillance was the product of FAA surveillance may itself be a complicated question, *see* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, http://nyti.ms/1sBRGDr (discussing disagreement within DOJ about the meaning of the phrase "derived from"); and if the FISA applications was indeed the product of FAA surveillance, the question of the lawfulness of that surveillance would involve additional layers of complexity. In these circumstances, Section 1806 must be construed to require disclosure of FISA materials, and the Seventh Circuit erred in concluding otherwise.

As Judge Rovner observed in concurrence, the Seventh Circuit's construction of Section 1806 created tension or even conflict with this Court's jurisprudence, and in particular with *Franks*. *See* Pet. App. 29a ("As a practical matter, the secrecy

shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks*.").

Notably, however, Judge Rovner was not the first to observe this. To the contrary, many other courts have construed Section 1806 narrowly while noting that their construction of the statute creates tension or conflict with *Franks*. *See United States v. Huang*, 15 F. Supp. 3d 1131, 1142 (D.N.M. 2014) ("The Court acknowledges that without access to the FISA affidavit, Defendant is constrained from making an examination of the affidavit in the first place."); *United States v. Alwan*, 2012 WL 399154, at *9–10 (W.D. Ky. Feb. 7, 2012) ("Hammadi cannot offer any proof that statements in the FISA applications were false or were deliberately or recklessly made because Hammadi has not been able to examine the applications. The Court is cognizant of the substantial difficulties Hammadi has encountered in trying to assert a *Franks* violation."); *United States v. Mehanna*, 2011 WL 3652524, at *2 (D. Mass. Aug. 19, 2011) ("The Court recognizes the defendant's difficulty in making such a preliminary showing where the defendant has no access to the confidential FISA-related documents here."); *United States v. Kashmiri*, 2010 WL 4705159, at *5–6 (N.D. Ill. Nov. 10, 2010) ("The Court recognizes the frustrating position from which Defendant must argue for a *Franks* hearing. *Franks* provides an important Fourth Amendment safeguard to scrutinize the underlying basis for probable cause in a search warrant. The requirements to obtain a hearing, however, are seemingly unattainable by Defendant."); *United States v. Mubayyid*, 521 F.

Supp. 2d 125, 130–31 (D. Mass. 2007) ("The Court obviously recognizes the difficulty of defendants' position: because they do not know what statements were made by the affidavit in the FISA applications, they cannot make any kind of a showing that those statements were false."); *see also United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982) ("We appreciate the difficulties of appellants' counsel in this case."); *United States v. Hussein*, 2014 WL 1682845, at *2 (S.D. Cal. Apr. 29, 2014) ("The Court is aware that Defendant has been unable to review the FISA materials[.]"); *United States v. Abu–Jihaad*, 531 F. Supp. 2d 299, 311 (D. Conn. 2008) ("Since defense counsel has not had access to the Government's submissions they—quite understandably—can only speculate about their contents."), *aff'd*, 630 F.3d 102; *United States v. Hassoun*, 2007 WL 1068127, at *3–4 (S.D. Fla. Apr. 4, 2007) ("Defendants admit that their allegations are purely speculative, in that they have not been given the opportunity to review the classified applications.").

4. Section 1806 must be read more generously to allow for disclosure of FISA materials at least in the kinds of circumstances presented here. As an initial matter, a broader construction of the statute is mandated by the principle of constitutional avoidance. *See, e.g.*, *Hooper v. California*, 155 U.S. 648, 657 (1895) ("The elementary rule is that every reasonable construction must be resorted to in order to save a statute from unconstitutionality."); *New York v. United States*, 505 U.S. 144, 170 (1992) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems,

the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." (quoting *DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988))).

A broader construction of the statute would also be more consistent with the statute's text, structure, and legislative history. On its face, the statute allows defendants to move for disclosure of FISA materials; it envisions that the Attorney General may oppose disclosure in some cases but not others; it empowers district courts to order the disclosure of FISA materials even over the Attorney General's objection; and it empowers district courts to tailor disclosure to the circumstances of each case. The statute's text and structure make clear that Congress intended the disclosure of FISA materials to be more than merely a theoretical possibility. Indeed, there is a stark disconnect between the text of the statute and the fact that no defendant, in the 35 years FISA has been operative, has been able to obtain access to FISA materials under the statute.

The statute's legislative history confirms that Congress anticipated that FISA materials would be disclosed in cases involving especially complex issues of fact or law. The Senate Judiciary and Intelligence Committees explained that Congress sought to "strik[e] a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information." S. Rep. No. 604(I), 95th Cong., 1st Sess.

at 57, *reprinted in* 1978 U.S.C.C.A.N. 3959; S. Rep. No. 701, 95th Cong., 2d Sess. at 64, *reprinted in* 1978 U.S.C.C.A.N. 4033. The Committees also described factors that they expected courts to consider when applying the disclosure provisions. Disclosure would likely be warranted, they wrote, when questions about a FISA order's legality were "more complex." *Id.* Disclosure might be warranted because of the "volume, scope, and complexity" of the materials, or because of other factors, such as "indications of possible misrepresentations of fact." *Id.*; *see also Belfield*, 692 F.2d at 147–48 (discussing Congress's intent to require disclosure where questions of law may be complicated); *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987).

Thus, the prevailing construction of Section 1806 is not only in tension with this Court's constitutional jurisprudence, but unsupported by the statute's text and legislative history.

III. This Case Is an Appropriate Vehicle to Clarify the Circumstances in Which a Defendant Who Was Subject to FISA Surveillance Is Entitled to Examine FISA Materials

Petitioner's case presents an opportunity to reconcile Section 1806(f) with this Court's Fourth and Fifth Amendment jurisprudence. As noted above, many courts have remarked on the tension or conflict between the prevailing construction of Section 1806(f) and this Court's jurisprudence, and with *Franks* in particular. Although this Court's Fourth and Fifth Amendment jurisprudence guarantees defendants a meaningful opportunity to seek to

suppress evidence that was obtained unlawfully, the prevailing construction of Section 1806(f) is one that has barred disclosure of FISA materials in every FISA prosecution since 1978—and that has thereby deprived many defendants of the rights that the Constitution guarantees. In her concurrence below, Judge Rovner rightly noted that the conflict between the prevailing construction of Section 1806(f) and *Franks* demands resolution:

> My purpose in engaging in this discussion has been to acknowledge a problem that thus far has not been addressed as deeply as it should be by the judiciary. Thirty-six years after the enactment of FISA, it is well past time to recognize that it is virtually impossible for a FISA defendant to make the showing that *Franks* requires in order to convene an evidentiary hearing, and that a court cannot conduct more than a limited *Franks* review on its own. Possibly there is no realistic means of reconciling *Franks* with the FISA process. But all three branches of government have an obligation to explore that question thoroughly before we rest with that conclusion.

Pet. App. 50a–51a.

The very fact that no court—but for the district court below—has ever ordered disclosure under Section 1806(f) makes it unlikely that any court will do so in the future. This Court's intervention is necessary to re-align Section 1806(f) with its text and legislative history, and with this Court's constitutional jurisprudence.

That need is especially urgent since disclosures over the past two years have called into question whether judicial oversight of national security surveillance is adequate to prevent abuse and preserve the constitutional balance between liberty and security. *See* Adrian Croft, *Obama Says U.S. Needs to Win Back Trust After NSA Spying*, Reuters, May 25, 2014, http://reut.rs/1tcCJHq (quoting President Obama: "because of these revelations, there is a process that is taking place where we have to win back the trust, not just of governments, but more importantly of ordinary citizens, and that is not going to happen overnight"). Criminal defendants seek disclosure under Section 1806(f) in order to vindicate individual rights, but there is a broader societal interest in ensuring that the government's surveillance activities are subject to informed, adversarial review and constitutional challenge. Through Petitioner's case, this Court has the opportunity to provide guidance concerning the role that federal judges should play in ensuring that the government's surveillance practices are consistent with the Constitution.

Furthermore, the facts of this case demonstrate the importance of holding that Section 1806(f) requires disclosure where the surveillance of the defendant raises complex factual and legal questions and where the district court judge concludes, after *ex parte* review of the materials, that disclosure to security-cleared counsel would enhance the court's ability to adjudicate the legality of the surveillance. As discussed, Petitioner's case raises complex questions because there is evidence in the public record that the government used the FAA to monitor

Petitioner's communications; there is uncertainty about whether the government used FAA-derived evidence to obtain FISA orders; and the constitutionality of the FAA has never been adjudicated by any appeals court. If Petitioner's cleared counsel had access to the FISA materials, counsel would be in a position to make more informed arguments about the constitutionality of the government's surveillance of Petitioner and the admissibility of evidence derived from that surveillance.

CONCLUSION

For the foregoing reasons, the petition for writ of certiorari should be granted.

Respectfully submitted,

Thomas Anthony Durkin
COUNSEL OF RECORD
Janis D. Roberts
Joshua G. Herman
DURKIN & ROBERTS
2446 North Clark Street
Chicago, IL 60614
(312) 913-9300
TDURKIN@DURKINROBERTS.COM

John D. Cline
LAW OFFICE OF JOHN D. CLINE
235 Montgomery Street,
Suite 1070
San Francisco, CA 94104

Jameel Jaffer
Steven R. Shapiro
Patrick Toomey
Ashley M. Gorski
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004

Matthew R. Segal
Jessie J. Rossman
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MASSACHUSETTS
211 Congress Street,
3rd Floor
Boston, MA 02110

Harvey Grossman
ROGER BALDWIN FOUNDATION
OF ACLU, INC.
180 N. Michigan Ave,
Suite 2300
Chicago, IL 60601

COUNSEL FOR PETITIONER

December 31, 2014

APPENDIX TABLE OF CONTENTS

SUPPLEMENTAL OPINION OF THE SEVENTH CIRCUIT, REDACTED (JULY 29, 2014)

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff–Appellant,

v.

ADEL DAOUD,

Defendant–Appellee.

No. 14–1284

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division
No. 12 CR 723— Sharon Johnson Coleman, Judge

Before POSNER, KANNE, and ROVNER,
Circuit Judges.

Argued June 4 & June 9, 2014
Decided June 16, 2014

Supplemental Classified Opinion
Decided July 14, 2014

POSNER, Circuit Judge.

In our June 16 opinion reversing the district judge's order to disclose classified materials to defense counsel, we also held that the government's

investigation of the defendant did not violate the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 *et seq.* We promised to "issue a classified opinion explaining (as we are forbidden to do in a public document) these conclusions, and why therefore a remand to the district court is neither necessary nor appropriate." This is that opinion.

The FBI's investigation of the defendant was triggered [redacted]

[redacted]

the FBI's Chicago office immediately began investigating the defendant. Yahoo responded to a grand jury subpoena [redacted] confirming that the account [redacted] belonged to a "Mr. Adel Daoud." [redacted]

A few days later, an "online covert employee" of the FBI exchanged emails with [redacted] and thereby obtained his IP address; on [redacted] Comcast, responding to a grand-jury subpoena, confirmed that the IP address was associated with a residential account at 2317 Westwood Drive, Hillside, Illinois—the defendant's address, according to the Illinois Secretary of State Division of Motor Vehicles database. [redacted]

[redacted]

The defendant argues that the evidence against him was "obtained or derived from electronic surveillance" that "was not lawfully authorized or conducted," 50 U.S.C. § 1806(g), and should therefore be suppressed. Lacking access to the warrant applications, he presents several conjectures about the warrants' possible illegality. We can restrict our analysis to the first FISA application, [redacted] *Cf. Wong Sun v. United States,* 371 U.S. 471, 83 S. Ct. 407 (1963).

The FISA applications are free of any procedural defects. The applications were "made by a federal officer and approved by the Attorney General," 50 U.S.C. § 1805(a)(1), each of them listing the name and background of the special agent submitting the application and each of them containing the signatures of the FBI Director or Deputy Director and the Assistant Attorney General for National Security. The government also proposed and followed the required "minimization procedures" to ensure that no more information than necessary was collected from the target of the electronic surveillance and that the information once obtained would not be shared with anyone lacking a "need to know" it. 50 U.S.C. § 1805(a)(3); *see also* § 1801(h). The Foreign Intelligence Surveillance Court has already approved standing minimization procedures that are incorporated into each surveillance application. [redacted] And finally each of the applications "contains all statements and certifications required by section 1804." § 1805(a)(4); *see also* § 1804(a)(1)–(9).

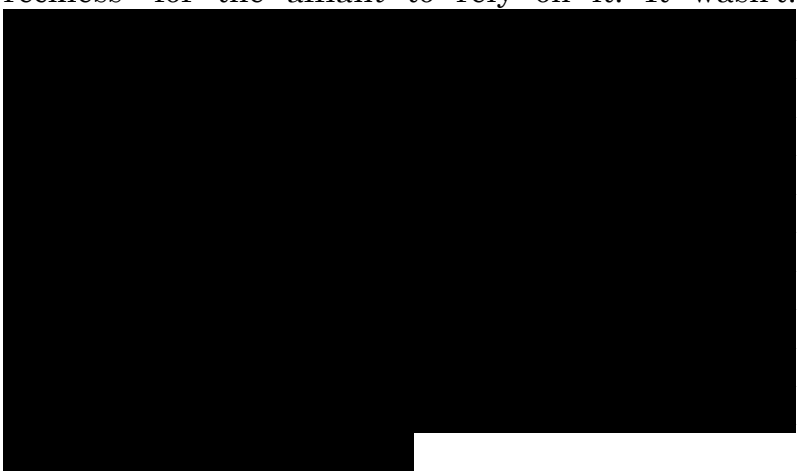
Like any search warrant, a FISA application must be supported by probable cause. But FISA doesn't require the government to show probable cause to believe that the target of the proposed surveillance may be engaged in criminal activity; rather, it requires only probable cause to believe that the target is an "agent of a foreign power." 50 U.S.C. §§ 1801(b), 1805(a)(2). The term is somewhat misleading; an "agent of a foreign power" needn't be

a KGB spy. Rather, anyone—even if a United States citizen—who "knowingly engages in . . . international terrorism, or in activities that are in preparation therefor, for or on behalf of" a "group engaged in international terrorism" qualifies. 50 U.S.C. §§ 1801(a)(4), (b)(2)(C); *e.g.*, *United States v. Aldawsari,* 740 F.3d 1015, 1018–19 (5th Cir.2014). And anyone who knowingly aids, abets, or conspires with an agent in furtherance of such activities is also deemed an agent of a foreign power. 50 U.S.C. § 1801(b)(2)(E).

The FISA applications contain ample evidence to support a finding of probable cause. [redacted] It would have been irresponsible of the FBI *not* to have launched its investigation of the defendant [redacted]

The defendant suggests that the applications may contain intentional or reckless material falsehoods, *see Franks v. Delaware,* 438 U.S. 154, 98 S. Ct. 2674 (1978), in violation of the Fourth Amendment. *Franks* however made clear that "the deliberate falsity or reckless disregard [for the truth] whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant." *Id.* at 171, 98 S. Ct. 2674. So even if the defendant is right to say that the [redacted] intelligence that triggered the

FBI's investigation may be based on "multiple-level hearsay, rumor, surmise, and speculation," all that matters is whether it was unreasonable—in fact reckless—for the *affiant* to rely on it. It wasn't.



Next, the defendant suggests that the primary purpose of the surveillance may have been to obtain evidence of *domestic* criminal activity, which is not authorized by FISA. *See United States v. Belfield,* 692 F.2d 141, 147 (D.C.Cir.1982). The

disposes of this possible objection.

Finally the defendant suggests that in the spring of 2012 he had been conducting online research for a term paper on Osama bin Laden, and that this online research—which is protected by the First Amendment—may have triggered the government's investigation. If that's the case, then the electronic surveillance wouldn't have been authorized, because "no United States person [such as the defendant] may be considered . . . an agent of a foreign power solely upon the basis of activities protected by the first amendment." 50 U.S.C.

§ 1805(a)(2)(A). (Relatedly, the defendant suggests that the surveillance may be illegal for the additional reason that it would have taken place before the defendant had turned 18.) This is a non sequitur; there's no age restriction in FISA [redacted].

The defendant suggests that at least some of the evidence against him may have been obtained as a result of surveillance conducted pursuant to the FISA Amendments Act of 2008 (FAA), Pub.L. 110–261, 122 Stat. 2436 (2008), and if so he's entitled to be notified of that fact. Unlike a traditional FISA application for electronic surveillance, an application under the FAA "does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power" as long as the surveillance targets "non-U.S. persons located abroad." *Clapper v. Amnesty International USA,* ___U.S.___, 133 S. Ct. 1138, 1144 (2013). The FAA also "eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis." *Id.* at 1156 (dissenting opinion); *see also* 50 U.S.C. § 1881a(g). In short, it's *easier* for the

government to conduct lawful electronic surveillance under the FAA than under the traditional FISA provisions.

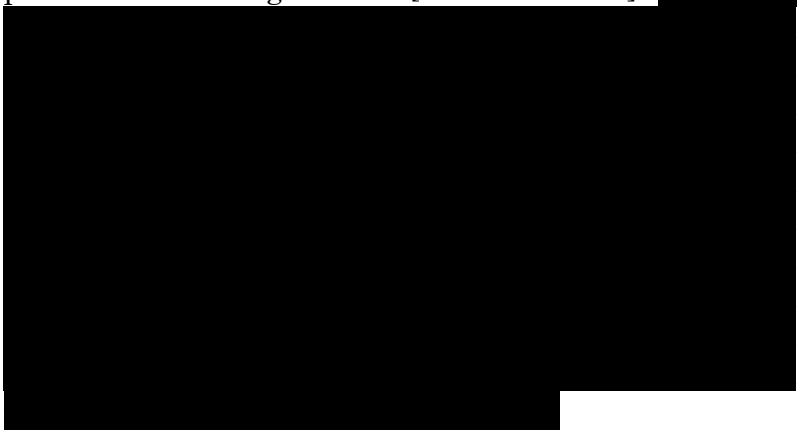
Since as we said the government has met FISA's tougher standard. [redacted]

The defendant's challenge relies primarily on a December 27, 2012 Senate floor speech by Senator Feinstein, who said: "There have been 16 individuals arrest[ed] just this year alone. Let me quickly just review what these plots were. And *some of them* come right from this program [meaning, the FAA]. The counter-terrorism come[s]—and the information came right from this program. And again, if members want to see that, they can go and look in a classified manner. . . . Fourth, a plot to bomb a downtown Chicago bar. . . . " www.c-span.org/video/?c4467868 (emphasis added) (visited July 11, 2014).

The referenced "plot" is obviously the defendant's, and because the Senator used the examples to support the reauthorization of the FAA, the defendant not unreasonably interpreted her remarks to mean that the FAA had been used in *his* case. But an equally

reasonable interpretation of the Senator's remarks is that she was merely saying that the defendant was one of the 16 individuals who had been arrested in 2012, *some* of whom had been arrested on the basis of such information. The Senate's Legal Counsel confirmed in a letter to defense counsel that "Senator Feinstein did not state, and did not mean to state, that FAA surveillance was used in any or all of the nine cases she enumerated, including [the defendant's] case, in which terrorist plots had been stopped. . . . Rather, her purpose in reviewing several recent terrorism arrests was to refute the 'view by some that this country no longer needs to fear attack.'"

We asked the government after the classified oral argument to tell us whether "any FAA information play[ed] any role, no matter how minimal, in the investigation of [the defendant] or the decision to pursue an investigation of [the defendant].



We close with a word on disclosure of the FISA material to defense counsel, which the Attorney General swore in an affidavit would "harm the national security of the United States." As we

pointed out in our June 16 opinion, counsel's obligation to zealously represent the defendant comes with a real risk of inadvertent or mistaken disclosure; the risk is particularly worrisome in a case involving sensitive information [redacted] The FISA applications in this case also revealed [redacted] the secrecy of which is unquestionably important to maintain.

To summarize, the FISA applications in this case are supported by probable cause to believe that

the defendant was an "agent of a foreign power," as FISA defines that term, and the information collected from the resulting surveillance should therefore not be suppressed.

OPINION OF THE SEVENTH CIRCUIT REVERSING THE ORDER OF THE DISTRICT COURT (JUNE 16, 2014)

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff–Appellant,

v.

ADEL DAOUD,

Defendant–Appellee.

No. 14–1284

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division.
No. 12 CR 723—Sharon Johnson Coleman, Judge.

Argued June 4 & June 9, 2014.*—
Decided June 16, 2014.

---

*The fact that we heard oral argument twice before issuing our decision is unusual and requires explanation. By inadvertence the device that makes a sound recording of the oral arguments of our cases was not turned on for the public argument in this case on June 4. (That argument was followed by a classified argument, which was recorded stenographically by a court reporter who has the necessary security clearance. Our present opinion pertains only to the public argument.) Recording, whether aural or stenographic, of oral arguments is not required by law; and the recordings are not required to be made

Before POSNER, KANNE, and ROVNER,
Circuit Judges.

POSNER, Circuit Judge.

The defendant, Adel Daoud, was indicted first in September 2012 for attempting to use a weapon of mass destruction and attempting to damage and destroy a building by means of an explosive, in violation of 18 U.S.C. §§ 2332a(a)(2)(D) and 844(i), and next in August 2013 for having, in addition, later solicited a crime of violence, murder for hire, and witness tampering, in violation of 18 U.S.C. §§ 373(a), 1958(a), and 1512(a)(1)(A), respectively.

The first indictment arose out of an investigation that began in May 2012 when Daoud, an 18–year–old American citizen and resident of Hillside, Illinois, a suburb of Chicago, joined an email conversation with two undercover FBI employees posing as terrorists who had responded to messages that he had posted online. The ensuing investigation, based in part on a series of surveillance warrants, yielded evidence that Daoud planned "violent jihad"—terrorist attacks in the name of Islam—and had discussed his plans with "trusted brothers." He expressed interest in committing such attacks in the United States, utilizing

---

public. Until our recording equipment was installed some years ago, no record was made by the court of the oral arguments. And initially the recordings were available only to the judges. Eventually the court decided to make them available to the public as well. Although under no legal obligation to conduct a second oral argument in this case, we decided to do so because the accidental failure to record the argument occurred in a high-profile case involving serious criminal charges.

bombmaking instructions that he had read both in *Inspire* magazine, an organ of Al Qaeda that is published in English, and through internet searches.

One of his FBI correspondents put him in touch with an undercover agent (a "cousin") whom the correspondent represented to be a fellow terrorist. After meeting six times with the "cousin," Daoud selected a bar in downtown Chicago to be the target of a bomb that the agent would supply him with. The agent told him the bomb would destroy the building containing the bar, and warned him that it would kill "hundreds" of people. Daoud replied: "that's the point."

On September 14, 2012, Daoud parked a Jeep containing the bomb in front of the bar. In a nearby alley, in the presence of the agent, he tried to detonate the bomb. Nothing happened, of course, because the bomb was a fake. Daoud was immediately arrested. It was while in jail a month later that, according to the second indictment, he tried to solicit someone to murder the undercover agent with whom he had dealt.

The government notified the defendant, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d)—sections of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 *et seq.*—that it intended to present evidence at his trial derived from electronic surveillance that had been conducted under the authority of the Act. Daoud responded through counsel with a motion seeking access to the classified materials submitted in support of the government's FISA warrant applications. Counsel hoped to show that the "evidence obtained or derived from such

electronic surveillance" had been based on "information [that] was unlawfully acquired" or that "the surveillance was not made in conformity with an order of authorization or approval," 50 U.S.C. § 1806(e), both being grounds for suppression.

The government filed two responses: a heavily redacted, unclassified response, accessible to Daoud and his lawyers, and a classified version, accessible only to the district court, accompanied by an unclassified statement by the Attorney General that disclosure of the classified material, or an adversarial hearing with respect to it, "would harm the national security of the United States"; the harm was detailed in a classified affidavit signed by the FBI's Acting Assistant Director for Counterterrorism.

The district judge studied the classified materials to determine whether they should be shown to the defendant's lawyers, who have security clearances at the level at which these materials are classified. The judge noted that counsel was seeking "disclosure of classified documents that are ordinarily not subject to discovery," that "no court has ever allowed disclosure of FISA materials to the defense," and that a court may order such disclosure only where "necessary" for "an accurate determination of the legality of the surveillance," 50 U.S.C. § 1806(f), or of the "physical search" if that was how the FISA materials were obtained. § 1825(g). Nevertheless, remarking that "the adversarial process is integral to safeguarding the rights of all citizens," that the Sixth Amendment presupposes "the right of the accused to require the prosecution's case to survive the crucible of meaningful adversarial testing," and that "the supposed national security interest at stake is not implicated where

defense counsel has the necessary security clearances," the judge ruled that "the probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel." And so she ordered the materials sought by defense counsel turned over to them. The order, though interlocutory, was appealable immediately, and the government appealed. 50 U.S.C. § 1806(h); 18 U.S.C. App. III § 7.

She acknowledged that the Attorney General's submission—stating that disclosure of the classified material, or an adversarial hearing with respect to it, "would harm national security"—had "trigger[ed] an *in camera, ex parte* procedure [in the district court] to determine whether the surveillance of the aggrieved person [Daoud] was lawfully authorized and conducted." FISA is explicit about this. It provides that "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, [the court shall] 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. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance *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).

So first the district judge must, in a non-public ("*in camera*"), nonadversarial ("*ex parte*") proceeding,

attempt to determine whether the surveillance was proper. If in attempting to determine this the judge discovers that disclosure to the defendant of portions of the FISA materials is "necessary," the judge may order disclosure, provided there is adequate security. The defendant's brief tries to delete the statutory requirement of sequential *ex parte in camera* district court analysis by a cropped quotation from the statute: "the court must review the FISA application, order, and related materials *ex parte* and *in camera,* unless 'disclosure [to the defendant] is necessary to make an accurate determination of the legality of the surveillance.'" The defendant's misreading of the statute would permit the district judge to avoid conducting an *ex parte* review if the defendant's lawyers believed disclosure necessary, since if the judge does not conduct the *ex parte* review she will have no basis for doubting the lawyers' claim of necessity. The statute requires the judge to review the FISA materials *ex parte in camera* in *every* case, and on the basis of that review decide whether any of those materials must be disclosed to defense counsel. The judge did not do that. She did not find that disclosure was necessary, only that it "may be necessary." Although she read the FISA materials and concluded that she was "capable of making such a determination [an 'accurate' determination, as is apparent from a previous sentence in her order] of the legality of the surveillance," she refused to make the determination, which if she was right in thinking she could make an accurate determination would have obviated the necessity for—and therefore the lawfulness of—disclosure of the classified materials to defense counsel.

The judge appears to have believed that adversary procedure is always essential to resolve contested issues of fact. That is an incomplete description of the American judicial system in general and the federal judicial system in particular. There are *ex parte* or *in camera* hearings in the federal courts as well as hearings that are neither or both. And there are federal judicial proceedings that though entirely public are nonadversarial, either partly or entirely. For example, a federal district judge presiding over a class action is required to determine the fairness of a settlement agreed to by the parties even if no member of the class objects to it. *Eubank v. Pella Corp.,* 753 F.3d 718, 720, 2014 WL 2444388, at *2 (7th Cir. June 2, 2014). And when in a criminal case the prosecutor and the defendant agree on the sentence to recommend, the judge must make an independent determination whether the sentence is appropriate. If, though it is within the range fixed by Congress, he thinks the agreed-upon sentence too harsh or too lenient, he is empowered (indeed required) to reject the agreed-upon sentence and impose a different one within the statutory range. *United States v. Siegel,* 753 F.3d 705, 710, 2014 WL 2210762, at *5 (7th Cir. May 29, 2014). Another familiar example of nonadversarial federal procedure involves the "*Anders* brief"—a brief in which a criminal defendant's lawyer states that the appeal is frivolous and therefore moves to be allowed to withdraw from representing the defendant. *See Anders v. California,* 386 U.S. 738, 87 S. Ct. 1396 (1967). If the appellate court agrees, his motion is granted and the appeal dismissed. Unless the defendant expresses disagreement with the position

taken by his lawyer in the *Anders* brief (the court always invites the defendant to respond to the brief but defendants often do not), there is no adversary process. Yet the court proceeds to make its own determination whether an appeal would be frivolous. If the court disagrees, it denies the lawyer's motion to withdraw and so retains the appeal.

Not only is federal judicial procedure not always adversarial; it is not always fully public. Child witnesses, especially in sexual abuse cases, are often allowed to testify behind a screen. Criminal defendants typically are allowed to conceal from the jury most or even all of their criminal history. (Notice that in such a case, and in many other cases, secrecy inures to the defendant's benefit.) Objections to questions to witnesses when sustained keep from the jury evidence that jurors might be very interested in. Documents placed in evidence may be redacted to conceal embarrassing material. Trade secrets—and classified materials are a form of "trade secret"—are routinely concealed in judicial proceedings. And of course judicial deliberations, though critical to the outcome of a case, are secret.

The propriety of government confidentiality is not limited to judicial proceedings. Though the Freedom of Information Act provides broad access to information collected by or generated within government, it has many exceptions. 5 U.S.C. § 552(b). The government's records of people's finances, collected by the Internal Revenue Service and other agencies, are secret. So are medical records of persons enrolled in Medicaid, Medicare, and the Veterans Administration's hospital system. Employment files for the millions of federal employees are secret, as are public

school teachers' evaluations of children, government social workers' judgments about their clients, and deliberations of a wide range of government officials, not limited to judges—for example, the doctrine of executive privilege shields many of the internal communications of executive-branch officials. The methods used by police to audit and investigate, to decide where to set up roadblocks and hide plainclothes officers, are secret, as are their communications with and the names of their confidential informants unless the informants testify.

Everyone recognizes that privacy is a legally protectable interest, and it is not an interest of private individuals alone. The Foreign Intelligence Surveillance Act is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation. Terrorism is not a chimera. With luck Daoud might have achieved his goal of indiscriminately killing hundreds of Americans—whom he targeted because, as he explained in an email, civilians both "pay their taxes which fund the government's war on Islam" and "vote for the leaders who kill us everyday."

Conventional adversary procedure thus has to be compromised in recognition of valid social interests that compete with the social interest in openness. And "compromise" is the word in this case. Daoud was first indicted almost two years ago. Defense counsel have been conducting discovery and have submitted extensive factual allegations to the district court. Those allegations—made in an extensive proffer by the defendant—were before the district

judge when she was considering whether to disclose any of the classified FISA materials to defense counsel, along with the factual allegations made by the government as the result of its investigation. It was her obligation to evaluate the parties' allegations in light of the FISA materials to determine whether she could assess the legality of those materials herself, without disclosure of them to Daoud's lawyers.

The defendant's lawyers place great weight on the difficulty of conducting a *Franks* hearing to determine the legality of a warrant to conduct FISA surveillance. *Franks v. Delaware,* 438 U.S. 154, 98 S. Ct. 2674 (1978), held that a defendant can challenge a search or arrest warrant on the ground that it was procured by a knowing or reckless falsehood by the officer who applied for the warrant. *Id.* at 155–56, 98 S. Ct. 2674. Defense counsel would like to mount such a challenge in this case. But that's hard to do without access to the classified materials on which the government relied in obtaining a warrant to obtain access to Daoud's communications. The drafters of the Foreign Intelligence Surveillance Act devised a solution: the judge makes the additional determination, based on full access to all classified materials and the defense's proffer of its version of events, of whether it's possible to determine the validity of the *Franks* challenge without disclosure of any of the classified materials to the defense. The judge in this case failed to do that.

She seems to have thought that any concerns about disclosure were dissolved by defense counsel's security clearances. She said that "the government had no meaningful response to the argument by defense counsel that the supposed national security

interest at stake is not implicated where defense counsel has the necessary security clearances"—as if disclosing state secrets to cleared lawyers could not harm national security. Not true. Though it is certainly highly unlikely that Daoud's lawyers would, Snowden-like, publicize classified information in violation of federal law, they might in their zeal to defend their client, to whom they owe a duty of candid communication, or misremembering what is classified and what not, inadvertently say things that would provide clues to classified material. Unless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction.

It's also a mistake to think that simple possession of a security clearance automatically entitles its possessor to access to classified information that he is cleared to see. (The levels of classification differ; someone cleared for Secret information is not entitled to access to Top Secret information.) There are too many leaks of classified information—too much carelessness and irresponsibility in the handling of such information—to allow automatic access to holders of the applicable security clearances. More than a million and a half Americans have security clearances at the Top Secret level, which is the relevant level in this case. Office of Management and Budget, "Suitability and Security Processes Review: Report to the President," Feb. 2014, p. 3, www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf

(visited June 14, 2014). Like the Fifth Circuit in *United States v. El–Mezain,* 664 F.3d 467, 568 (5th Cir.2011), "we are unpersuaded by the defendants' argument that the Government's interest [in confidentiality] is diminished because defense counsel possess security clearance to review classified material."

So in addition to having the requisite clearance the seeker must convince the holder of the information of the seeker's need to know it. If the district judge's threshold inquiry into whether Daoud's lawyers needed any of the surveillance materials revealed that they didn't, their security clearances would not entitle them to any of those materials. The statute says that disclosure of such materials to them must be "necessary"; even without that word (the vagueness of which in legal contexts is legendary, as lucidly explained in *Cellular Telecommunications & Internet Ass'n v. FCC,* 330 F.3d 502, 509–12 (D.C.Cir.2003)), the judge in this case would have had to determine the lawyers' need for the materials—more precisely, her need for them to have access to the materials so that she could make an accurate determination of the legality of the challenged surveillance. Rather than asserting such a need, she affirmed her capability of making an accurate determination without disclosing any classified materials to defense counsel. Because she was "capable" of making the determination, disclosure was not "necessary" under any definition of that word. We conclude regretfully that the judge thus disobeyed the statute.

Our own study of the classified materials has convinced us that there are indeed compelling reasons of national security for their being classified—that the government was being truthful in advising the district

judge that their being made public "would harm the national security of the United States"—and that their disclosure to the defendant's lawyers is (in the language of section 1806(f)) not "necessary" for "an accurate determination of the legality of the surveillance." So clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so.

Not only do we agree with the district judge that it is possible to determine the legality of the government's investigation of Daoud without disclosure of classified materials to his lawyers; our study of the materials convinces us that the investigation did not violate FISA. We shall issue a classified opinion explaining (as we are forbidden to do in a public document) these conclusions, and why therefore a remand to the district court is neither necessary nor appropriate.

One issue remains to be discussed. After the first oral argument, we held a brief *in camera* hearing at which questions were put by the panel to the Justice Department's lead lawyer on the case concerning the classified materials. Only cleared court and government personnel were permitted at that hearing. The defendant's lawyers, before leaving the courtroom as ordered, objected to our holding such a hearing and followed up their oral objection with a written motion. Their objecting to the classified hearing was ironic. The purpose of the hearing was to explore, by questioning the government's lawyer on the basis of the classified materials, the need for defense access to those materials (which the

judges and their cleared staffs had read). In effect this was cross-examination of the government, and could only help the defendant.

Defense counsel's written motion cites no authority for forbidding classified hearings, including classified oral arguments in courts of appeals, when classified materials are to be discussed. We don't think there's any authority it could cite. The propriety of such hearings was confirmed in *United States v. Sedaghaty,* 728 F.3d 885, 891 and n. 2 (9th Cir.2013); *cf. American Civil Liberties Union v. Department of Justice,* 681 F.3d 61, 66, 70 (2d Cir.2012). But we are granting the request of the defendant's lawyers for a redacted transcript of our classified hearing.

Finally, for future reference we suggest that when a district judge is minded to disclose classified FISA materials to defense counsel—a decision bound to precipitate an appeal by the government—the judge issue a classified statement of reasons, as it probably will be impossible to explain in an unclassified opinion all the considerations motivating her decision. In this case, however, our review of the materials persuades us both that there was no basis for disclosure and that a remand would be of no value.

The order appealed from is

REVERSED.

CONCURRING OPINION OF JUDGE ROVNER, SEVENTH CIRCUIT (JUNE 16, 2014)

ROVNER, Circuit Judge. Concurring.

I join the court's opinion in full. I write separately to address the difficulty of reconciling *Franks v. Delaware,* 438 U.S. 154, 155–56, 98 S. Ct. 2674, 2676 (1978), with a proceeding in which the defense has no access to the FISA application that resulted in court-authorized surveillance of the defendant. As the court has recognized, *ante* at 483, this is one of the principal arguments that Daoud made in support of his request for disclosure of the FISA application.

Franks holds that a search warrant must be voided and the fruits of the search excluded from evidence when (1) a defendant proves by a preponderance of the evidence that the affidavit on which the search warrant was based contained false statements that were either deliberately or recklessly made, and (2) the court determines that the remainder of the affidavit was insufficient by itself to establish probable cause. *Id.* at 155–56, 98 S. Ct. at 2676. The *Franks* framework applies to misleading omissions in the warrant affidavit (so long as they were deliberately or recklessly made) as well as to false statements. *E.g., United States v. McMurtrey,* 704 F.3d 502, 508–09 (7th Cir.2013) (collecting cases).

Daoud asserted that the government's FISA application might contain material misstatements or omissions; but, of course, because the application is classified and his counsel has not seen it, he could present this only as a possibility. He therefore made

a pro forma request for a *Franks* hearing, but argued principally that, without access to the FISA application, he could not make the preliminary showing that is ordinarily required before the court will conduct such a hearing. R. 52 at 18–19.

In making a blind request for a hearing and relief under *Franks,* Daoud is presented with the same conundrum that every defendant charged on the basis of FISA-acquired evidence encounters. A *Franks* motion is premised on material misrepresentations and omissions in the warrant affidavit; but without access to that affidavit, a defendant cannot identify such misrepresentations or omissions, let alone establish that they were intentionally or recklessly made. As a practical matter, the secrecy shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks* absent a patent inconsistency in the FISA application itself or a *sua sponte* disclosure by the government that the FISA application contained a material misstatement or omission. To date, courts have either overlooked the problem or acknowledged it without being able to identify a satisfactory workaround.

I believe it is time to recognize that *Franks* cannot operate in the FISA context as it does in the ordinary criminal case. To pretend otherwise does a disservice to the defendant and to the integrity of the judiciary. We must recognize both that the defendant cannot make a viable *Franks* motion without access to the FISA application, and that the court, which does have access to the application, cannot, for the most part, independently evaluate the accuracy of that application on its own without the defendant's

knowledge of the underlying facts. Yet, *Franks* serves as an indispensable check on potential abuses of the warrant process, and means must be found to keep *Franks* from becoming a dead letter in the FISA context. The responsibility for identifying a solution lies with all three branches of government, but as the branch charged with applying *Franks,* the duty falls to the judiciary to acknowledge the problem, make such accommodations as it can, and call upon the other branches to make reforms that are beyond our power to implement.

Toward that end, I think it useful to devote some attention to the holding and rationale of *Franks,* what it requires of the defendant in the ordinary criminal case, what courts have said about *Franks* in the FISA context, how *ex parte, in camera* proceedings hobble the *Franks* inquiry, and possible solutions to the problem.

1.

It was in *Franks* that the Supreme Court first acknowledged the right of a criminal defendant to attack the veracity of the affidavit underlying a search warrant and to have the fruits of the search suppressed if the warrant would not have issued but for misrepresentations made in the affidavit. Prior to that holding, although a majority of courts had come to the conclusion that such challenges should be permitted, there remained a division of authority on this point at both the federal and state levels. *See id.* at 159–60 nn. 3–4 & App. B, 98 S. Ct. at 2678 nn. 3–4 & App. B; (collecting conflicting rulings). In *Franks* itself, the Delaware Supreme Court had altogether foreclosed impeachment of the warrant affidavit,

reasoning in part that it was "the function of the issuing magistrate to determine the reliability of information and credibility of affiants in deciding whether the requirement of probable cause has been met" and that "[t]here has been no need demonstrated for interfering with this function." *Franks v. State,* 373 A.2d 578, 580 (Del.1977), *rev'd,* 438 U.S. 154, 98 S. Ct. 2674 (1978). The United States Supreme Court resolved the conflict in favor of permitting impeachment, holding that where a defendant can establish that the warrant affiant made intentional or reckless material misstatements to the issuing judge, the results of the search must be suppressed if the remainder of the warrant would have been insufficient to establish probable cause. *Id.* at 155–56, 98 S. Ct. at 2676.

The *Franks* Court rested its holding on the Warrant Clause of the Fourth Amendment:

> In deciding today that, in certain circumstances, a challenge to a warrant's veracity must be permitted, we derive our ground from language of the Warrant Clause itself, which surely takes the affiant's good faith as its premise: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation. . . . " Judge Frankel . . . put the matter simply: "[W]hen the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a *truthful* showing" (emphasis in original). This does not mean "truthful" in the sense that every fact recited in the warrant affidavit is necessarily correct, for probable

> cause may be founded upon hearsay and upon information received from informants, as well as upon information within the affiant's own knowledge that sometimes must be garnered hastily. But surely it is to be "truthful" in the sense that the information put forth is believed or appropriately accepted by the affiant as true. It is established law that a warrant affidavit must set forth particular facts and circumstances underlying the existence of probable cause, so as to allow the magistrate to make an independent evaluation of the matter. . . . Because it is the magistrate who must determine independently whether there is probable cause, it would be an unthinkable imposition upon his authority if a warrant affidavit, revealed after the fact to contain a deliberately or reckless[ly] false statement, were to stand beyond impeachment.

438 U.S. at 164–65, 98 S. Ct. at 2681 (citations omitted). Later in its opinion, in the course of addressing Delaware's objections to any after-the-fact inquiry into the veracity of the warrant affidavit, the Court explained further why it rejected a rule that would foreclose any attempt to challenge the accuracy of the affidavit:

> [A] flat ban on impeachment of veracity could denude the probable-cause requirement of all real meaning. The requirement that a warrant not issue "but upon probable cause, supported by Oath or affirmation," would be reduced to a nullity if a police officer was

> able to use deliberately falsified allegations to demonstrate probable cause, and, having misled the magistrate, then was able to remain confident that the ploy was worthwhile. It is this specter of intentional falsification that, we think, has evoked such widespread opposition to the flat non-impeachment rule from the commentators, from the American Law Institute in its Model Code of Pre–Arraignment Procedure, from the federal courts of appeals, and from state courts.

438 U.S. at 168, 98 S. Ct. at 2682–83 (citations & footnote omitted).

2.

Although *Franks* allows a defendant to challenge the truthfulness of a warrant affidavit, he must surmount a significant threshold before the court is obliged to conduct an evidentiary hearing and to decide whether the search warrant was the product of an intentionally or recklessly false or misleading affidavit. In his *Franks* motion, the defendant must make a "substantial preliminary showing" that he is entitled to relief. *Id.* at 155, 98 S. Ct. at 2676. This requires him to do much more than point out inaccuracies in the warrant affidavit.

> There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to

> cross-examine. There must be allegations of a deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient. The deliberate falsity or reckless disregard whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant. Finally, if these requirements are met, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required. On the other hand, if the remaining content is insufficient, the defendant is entitled, under the Fourth and Fourteenth Amendments, to his hearing. Whether he will prevail at that hearing is, of course, another issue.

Id. at 171–72, 98 S. Ct. at 2684–85 (footnote omitted).

The "substantial preliminary showing" that *Franks* requires of the defendant is thus an onerous one. *See, e.g., McMurtrey,* 704 F.3d at 509; *United States v. Johnson,* 580 F.3d 666, 670 (7th Cir.2009); *United States v. Swanson,* 210 F.3d 788, 790 (7th

Cir.2000). Consequently, although *Franks* motions are standard fare in criminal cases, evidentiary hearings are granted infrequently. Nonetheless, hearings do occur with a modicum of regularity. *See, e.g., United States v. Spears,* 673 F.3d 598, 602–3 (7th Cir.), *cert. denied,* ___U.S.___, 133 S. Ct. 232, 184 (2012); *United States v. Clark,* 668 F.3d 934, 938–39 (7th Cir.2012); *United States v. Wilburn,* 581 F.3d 618, 621–22 (7th Cir.2009); *United States v. Merritt,* 361 F.3d 1005, 1010–11 (7th Cir.2004), *cert. granted & judgment vacated on other grounds,* 543 U.S. 1099, 125 S. Ct. 1024 (2005); *United States v. Whitley,* 249 F.3d 614, 617–19 (7th Cir.2001). Cases in which a motion to suppress is ultimately granted after such a hearing are even more uncommon, but they too occur. *See, e.g., United States v. Brown,* 631 F.3d 638, 649–50 (3d Cir.2011) (affirming suppression); *United States v. Foote,* 413 F.3d 1240, 1244 (10th Cir.2005) (noting but not ruling on partial suppression ordered by district court); *United States v. Wells,* 223 F.3d 835, 839–40 (8th Cir.2000) (affirming suppression); *United States v. Hall,* 113 F.3d 157, 159–61 (9th Cir.1997) (affirming suppression).

Despite the high bar to relief that *Franks* imposes, it has proven to be more than a lofty statement of principle that is often recited but in practice never results in relief. My experience as both a trial and appellate judge has convinced me that it is a vital part of the criminal process that subjects warrant affidavits to useful adversarial testing, and occasionally, if not often, results in the suppression of evidence seized as a result of the false or misleading warrant application, as *Franks* itself envisioned. 438

U.S. at 156, 98 S. Ct. at 2676. (Whether the same or a different form of relief would be appropriate in a case involving alleged terrorism is an issue that must be reserved for a case that presents it: To the best of my knowledge, no defendant has yet succeeded in getting to a *Franks* hearing in a criminal prosecution resulting from FISA surveillance.) And, no doubt, the prospect of a *Franks* hearing and the possibility of suppression serves as a meaningful deterrent to an overzealous law enforcement official who might be tempted to present a misleading account of the facts to the judge from whom he seeks a warrant.

3.

This court's opinion in *United States v. Ning Wen,* 477 F.3d 896, 897–98 (7th Cir.2007), makes clear that a FISA order qualifies as a warrant for purposes of the Fourth Amendment even if it authorizes only the interception of electronic communications as opposed to a physical search; and it has been widely assumed, if not affirmatively stated, in the decisions of other courts that *Franks* applies to FISA applications. *See, e.g., United States v. El–Mezain,* 664 F.3d 467, 570 (5th Cir.2011), *cert. denied,* ___U.S.___, 133 S. Ct. 525 (2012); *United States v. Abu–Jihaad,* 630 F.3d 102, 130–31 (2d Cir.2010); *United States v. Damrah,* 412 F.3d 618, 624–25 (6th Cir.2005); *United States v. Duggan,* 743 F.2d 59, 77 n. 6 (2d Cir.1984), *superseded on other grounds by statute as recognized in Abu–Jihaad,* 630 F.3d at 119–20; *United States v. Hussein,* 2014 WL 1682845, at *2 (S.D.Cal. Apr. 29, 2014); *United States v. Huang,* ___F. Supp.3d___, ___, 2014 WL 1599463, at *8 (D.N.M. Apr. 22, 2014); *United States v. Omar,*

2012 WL 2357734, at *3 & n. 1 (D.Minn. June 20, 2012); *United States v. Mehanna,* 2011 WL 3652524, at *2 (D.Mass. Aug. 19, 2011); *United States v. Kashmiri,* 2010 WL 4705159, at *5–*6 (N.D.Ill. Nov. 10, 2010); *United States v. Gowadia,* 2009 WL 1649714, at *3 (D.Hawai'i June 8, 2009); *United States v. Mubayyid,* 521 F. Supp.2d 125, 130–31 (D.Mass.2007); *United States v. Hassoun,* 2007 WL 1068127, at *3–*4 (S.D.Fla. Apr. 4, 2007). In this case, the government likewise assumes that *Franks* applies to the FISA context; it certainly does not argue to the contrary. *See* R. 73 at 43–47 (contending to district court that Daoud had not made a sufficient showing to trigger a *Franks* hearing, but making no argument that *Franks* does not apply in the FISA context).

4.

However, notwithstanding the presumed applicability of *Franks* to the FISA framework, defendants in FISA cases face an obvious and virtually insurmountable obstacle in the requirement that they make a substantial preliminary showing of deliberate or reckless material falsehoods or omissions in the FISA application without having access to the application itself. *Franks,* as I have discussed, requires such a showing before the court is obliged to convene an evidentiary hearing. And the necessary first step in that showing is to identify specific portions of the warrant affidavit that the defendant believes are false or misleading. *Franks,* 438 U.S. at 171, 98 S. Ct. at 2684.

In the typical criminal case, the defendant has access to the warrant affidavit. Coupled with his own

knowledge of what he or his accomplices said and did, the defendant can at least show that the government's affiant misstated or omitted facts pertinent to the probable cause determination—although he is, of course, required to go further and give the court reason to believe that the misstatement or omission was deliberate or reckless, *see id.* But without access to the FISA application, the defendant has no idea how the government represented the facts to the Foreign Intelligence Surveillance Court ("FISC"), let alone whether and how the government may have misstated the facts in some way. Practically speaking, the defense can only make a blind suggestion that there is a possibility that the FISA application may contain false statements or omissions and that a *Franks* hearing may be necessary, and cite this possibility as a reason for ordering disclosure. That is essentially what Daoud did here.

Some courts have acknowledged the inherent difficulty that defendants face without access to the FISA application; but those courts have insisted nonetheless that defendants must somehow make the same preliminary showing—that the government presented a distorted set of facts to the judge issuing the warrant—that *Franks* would require in the usual criminal case. The court's remarks in *Kashmiri* represent a thoughtful example:

> The Court recognizes the frustrating position from which Defendant must argue for a *Franks* hearing. *Franks* provides an important Fourth Amendment safeguard to scrutinize the underlying basis for probable cause in a search warrant. The requirements to obtain a hearing, however, are

> seemingly unattainable by Defendant. He does not have access to any of the materials concerning the FISA application or surveillance; all he has is notice that the government plans to use this evidence against him.
>
> Nevertheless, to challenge the veracity of the FISA application, Defendant must offer substantial proof that the FISC relied on an intentional or reckless misrepresentation by the government to grant the FISA order. The quest to satisfy the *Franks* requirements might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility. If Defendant obtains substantial proof that the FISC relied upon an intentional or recklessly false statement to approve the FISA order, he could obtain a hearing. . . .

2010 WL 4705159, at *6. *See also United States v. Alwan,* 2012 WL 399154, at *9–*10 (W.D.Ky. Feb. 7, 2012) (quoting *Kashmiri*); *Mehanna,* 2011 WL 3652524, at *2 ("The Court recognizes the defendant's difficulty in making such a preliminary showing where the defendant has no access to the confidential FISA-related documents here."); *United States v. Abu–Jihaad,* 531 F. Supp.2d 299, 311 (D.Conn.2008) ("Since defense counsel has not had access to the Government's submissions they—quite understandably—can only speculate about their contents."), *j. aff'd,* 630 F.3d 102; *Mubayyid,* 521 F. Supp.2d at 131

(see quoted passage below); *Hassoun,* 2007 WL 1068127, at *4 ("Defendants admit that their allegations are purely speculative, in that they have not been given the opportunity to review the classified applications.").

I note that in *Mubayyid,* the court expressly rejected this difficulty as a ground sufficient to warrant disclosure of the FISA application to the defense:

> The Court obviously recognizes the difficulty of defendants' position: because they do not know what statements were made by the affidavit in the FISA applications, they cannot make any kind of a showing that those statements were false. *see Belfield,* 692 F.2d at 148. Nonetheless, it does not follow that defendants are entitled automatically to disclosure of the statements. The balance struck under FISA—which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards—would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation.

521 F. Supp.2d at 131 (citing *United States v. Belfield,* 692 F.2d 141, 148 (D.C.Cir.1982) (expressing sympathy for similar difficulty defendant would have in attempting to show case was so complex that disclosure of FISA materials is warranted)). The *Mubayyid* court went on to note that Congress was

aware of the difficulties posed to the defense by a presumption against disclosure of FISA materials, but nonetheless "'chose to resolve them through means other than mandatory disclosure.'" *Id.* (quoting *Belfield,* 692 F.2d at 148).

One tactic that some defendants have attempted in order to trigger either a *Franks* hearing, or disclosure of the FISA materials so that the defense can make a proper preliminary showing under *Franks,* is to cite reports which take note of various misrepresentations that have been made to the FISC over the years and which have been confessed by the government after the fact. These disclosures, defendants reason, demonstrate that the possibility of a material misrepresentation or omission in the FISA application is more than a theoretical one. Most relevant in this regard is *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* 218 F. Supp.2d 611, 620 (Foreign Int.Surv.Ct.2002), *abrogated by In re Sealed Case,* 310 F.3d 717 (For.Intel.Surv.Ct.Rev.2002), in which the court recounted the government's revelation that 75 prior FISA applications related to major terrorist attacks directed against the United States contained misstatements and omissions of material facts (concerning such topics as whether the target of FISA surveillance was under criminal investigation, whether overlapping criminal and intelligence investigations were being appropriately compartmentalized in terms of information-sharing, and the prior relationship between the FBI and the FISA target). That disclosure led the FISC to bar one FBI agent from ever appearing before the court again as a FISA affiant. 218 F. Supp.2d at 621. Daoud has relied on this opinion

and others to demonstrate why disclosure of the FISA application to the defense is warranted for purposes of assessing the truthfulness of the application and, if discrepancies are found, to make the substantial preliminary showing that *Franks* requires. *See* R. 52 at 24–26.

Pointing to prior instances of falsehoods may be useful as a means of demonstrating a need for a *Franks* procedure or an equivalent in the FISA context, but it is of little use in satisfying the *Franks* standard, as it sheds no light on the truth or falsity of the particular FISA application under review. *See, e.g., Hassoun,* 2007 WL 1068127, at *4. Nor does it substantiate the necessity of disclosure of a FISA application in a particular case, unless there is reason to think that the FISA affiant is one who has been found to have made misleading applications before. *See id.* (noting the government's representation that the affiant was not the one who had been barred from appearing before the FISC).

A potential alternative was addressed by both the government and the members of the court at the oral arguments in this case. Although a defendant may not know what specific allegations were made in the FISA application, he necessarily does know what he has done and said. A savvy defense attorney might be able to surmise from the materials produced in discovery roughly when FISA surveillance began and what general types of information the government likely relied on in its warrant application. Counsel could in turn ascertain from his client which of his actions and statements—and those of his accomplices—the government might have known about and relied on to establish probable cause before the FISC.

In theory, the defense could present that information to the court and the court could compare the defense information with the representations in the FISA application and see if there are any important differences that might implicate the FISC's probable cause determination. Any such discrepancies might be grounds for disclosure of the FISA application to the defense so that it might attempt to make a proper *Franks* showing.

However, there are multiple problems posed by this scenario. To begin, rather than being able to rebut specific representations in the application, the defendant would have to supply the court with a narrative of his own conduct.[1] In doing so, the defendant would run the risk that he might disclose inculpatory facts about himself or an accomplice of which the government was not previously aware.[2]

Second, it will often be difficult for a defendant to recall and reconstruct all of the many communications and statements that the FISA application may have relied on to establish probable cause. Where it seems obvious that a discrete and recent event triggered a FISA application (something like the 2013 bombing at the Boston marathon, for example), recollecting and documenting a defendant's

---

[1] I am assuming that, as with a defendant's testimony in support of a motion to suppress, the defendant's narrative could not be introduced against him at trial on the issue of guilt over his objection. *See Simmons v. United States,* 390 U.S. 377, 394, 88 S. Ct. 967, 976 (1968).

[2] Permitting the defendant to submit his narrative *ex parte* for review by the court *in camera* presumably would resolve that problem.

acts and statements before and after that event may present a straightforward task. But in the modern era, people have at their disposal an almost unlimited means of communicating (phone, text, email, and all manner of social media), and young people like Daoud are often parties to many dozens of such communications per day. *See, e.g.,* Amanda Lenhart, Pew Research Center, *Teens, Smartphones & Texting* (Mar. 19, 2012) ("The median number of texts . . . sent on a typical day by teens [was] 60 in 2011."), available at http://pewinternet.org/Reports/2012/Teens-and-smartphones.aspx (last visited June 12, 2014). Recalling everything that one might or might not have said in the vast universe of his electronic chatter—and likewise what his accomplices have said—would pose a daunting task for anyone not gifted with total recall.

Third, a narrative-based approach allows for manipulation of the court, by giving the defense an incentive to present the most exculpatory (and incomplete) version of his actions and statements in order to maximize the chances that the court will order disclosure of the FISA application. If the defendant's threshold burden is to convince the court simply that the application may not have accurately described the defendant's actions, then his best shot at carrying that burden is to present the most self-serving version of events that he can without outright lying to the court. Balance and candor would work against him, because the more inculpatory things he acknowledges, the more likely it is that the court will conclude there is no material factual dispute justifying disclosure of the FISA application—

that the gist of the FISA application is consistent with the gist of the defendant's factual narrative.

Setting that point aside, let us suppose that a defendant in good faith presents a counter-narrative of the facts that convinces the court that disclosure of the FISA application is appropriate so that defense counsel may further pursue a *Franks* claim. It should be noted that producing the application to security-cleared defense counsel would pose the same risk of inadvertent disclosure to the defendant, and possible injury to national security, that the government has cited in challenging the disclosure that was ordered in this case.

More to the point, putting a copy of the FISA application in the defense counsel's hand would not necessarily enable a truly adversarial and robust *Franks* process. The defendant's attorney would not be authorized to disclose any classified material to his or her client; so the attorney would not be able to examine each material statement in the FISA application and discuss with the client whether it is accurate from the client's perspective. Even by asking the client generic, non-leading questions, counsel might inadvertently tip off the client to the classified evidence or sources the government may have relied on in the FISA application. And yet it would be difficult, if not impossible, for counsel to test the accuracy of the FISA application *without* disclosing the classified material to the client. In the end, the defense might be just as hamstrung in pursuing a *Franks* motion *with* disclosure of the FISA application to defense counsel as it would be *without* such disclosure.

Finally, even if it were possible for a defendant to make a preliminary *Franks* showing despite these obstacles, in cases involving sensitive information (which is most FISA cases, I would think), one wonders whether there could realistically be the sort of full-fledged, adversarial *Franks* hearing that takes place in a more typical criminal case, *cf. United States v. Whitley, supra,* 249 F.3d at 617–19 (recounting the extensive testimony bearing on defendant's *Franks* motion), even if the hearing were conducted in secrecy. Such a hearing would potentially expose the government's sources and methods of investigation to scrutiny that might jeopardize national security.

5.

Without access to the FISA application, it is doubtful that a defendant could ever make a preliminary showing sufficient to trigger a *Franks* hearing. The court in *Kashmiri* said that "[t]his perceived practical impossibility to obtain a hearing- . . . does not constitute a legal impossibility," 2010 WL 4705159, at *6, but it is not clear to me why this is so. It seems to me that only if the government itself somehow disclosed to the court or to the defense a material misrepresentation or omission in the FISA application, the court itself noticed a patent inconsistency in the application and pursued it, or a court reviewing many such applications noticed a suspicious pattern, could that showing be made. Those instances will be rare indeed, and they will occur wholly independently of the adversarial process that *Franks* envisions.

What courts sometimes say is that they have conducted their own careful review of the FISA materials and discovered no material misrepresentations or omissions in the FISA application. Thus, the *Kashmiri* court, after noting the difficulty the defendant would have in making the threshold showing that *Franks* requires, noted that it had "already undertaken a process akin to a *Franks* hearing through its *ex parte, in camera* review of the FISA materials" and detected no basis for further inquiry under *Franks*. 2010 WL 4705159, at *6 (citing 50 U.S.C. § 1806(f)). *See also Gowadia,* 2009 WL 1649714, at *3; *Abu–Jihaad,* 531 F. Supp.2d at 311–12.

Yet, although a court may be able to discover inconsistencies in the FISA materials, its ability to discover false statements and omissions is necessarily limited, as it has only the government's version of the facts. *Franks* itself recognizes that an *ex parte* inquiry into the veracity of the warrant affidavit is necessarily "less vigorous" than an adversarial hearing, as the judge "has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations." 438 U.S. at 169, 98 S. Ct. at 2683. The defendant is in the best position to know whether the government's version of events is inaccurate, as the defendant knows what he said and did, when, where, and to whom, and the defendant will often know the same about what his accomplices said and did.

If disclosure of the FISA application is to be the exception rather than the rule, then we must look for a means of ensuring that FISA affiants act in good faith and that the Fourth Amendment's probable-

cause requirement is not "denude[d] . . . of all real meaning." *Franks,* 438 U.S. at 168, 98 S. Ct. at 2682.

6.

I indicated earlier that I view it as mistaken to believe that a judge will be able on his or her own to ferret out any potential misrepresentations or omissions in the FISA application, given that the judge lacks a defendant's knowledge as to the facts underlying the application and has only the government's version of the facts as a reference point. There may be a subset of FISA cases, however, in which a judge could make a meaningful effort to confirm the accuracy of the application and thus serve the same interest in ensuring truth and candor in the warrant process that a *Franks* motion serves. These would be cases in which the FISA application is based in part on a defendant's documented statements. If, for example, the defendant has communicated his terrorist sympathies or plans in an email or a text to someone who turns a copy over to the government, or has posted such thoughts online, as the criminal complaint in this case notes that Daoud did (*see* R. 1 at 5 ¶ 7), and those statements are cited in the FISA application, the court could ask the government to produce complete copies of those statements for review *in camera.* Having those statements in hand would enable the court to verify that they were fairly recounted in the FISA application—both in the sense that the defendant was not misquoted and in the sense that the government did not omit portions of a statement that were critical for context. Taking that step would permit the court to conduct something akin to a *Franks* inquiry albeit without defense

input—perhaps something very much like the district court in *Kashmiri* referenced. 2010 WL 4705159, at *6.

Even such a modest step may strike some as a departure from the judge's usual detached role, and indeed it does require a judge to act as something more than a passive umpire. But it strikes me as a reasonable measure that respects both the national security interest as well as the practical obstacles that the defense faces in pursuing a *Franks* motion without access to those materials. As Judge Posner has pointed out today, there are any number of proceedings which are not wholly adversarial and which call on the court to exercise its judgment independently of the arguments presented to it. *Ante* at 482–83. To my mind, a *Franks* motion filed in a case involving FISA surveillance presents just such a situation, given that the defense cannot litigate that motion in the usual way. The court, which has unrestricted access to the FISA application, can make limited and reasonable efforts to do what the defense cannot: determine if the face of the FISA application is consistent with whatever documented statements of the defendant (or his accomplices) that the government might have in its possession.

There may be other steps that the judge can take to try and confirm the accuracy of the FISA application, but my essential point is this: courts cannot continue to assume that defendants are capable of carrying the burden that *Franks* imposes when they lack access to the warrant application that is the starting point for any *Franks* inquiry. Courts must do what they can to compensate for a defendant's ignorance as to what the FISA

application contains. Otherwise, *Franks* will persist in name only in the FISA setting.

Beyond this, it remains for Congress and the Executive Branch to consider reforms that might address some of the concerns I have raised here. If, as a pragmatic matter, *Franks* cannot function as a check on potential abuses of the warrant process in FISA cases, then there may be other institutional means of addressing the Fourth Amendment and due process rights that *Franks* is meant to protect in the standard criminal setting. Privacy concerns, for example, have resulted in multiple proposals before Congress calling for the creation of a "Special Advocate," with appropriate security clearance, whose job it would be to serve as a privacy advocate and to oppose the government in certain FISC proceedings.[3] The practical obstacles to impeaching the veracity of FISA applications warrant exploration of comparable measures that respect the spirit, if not the letter, of *Franks.*

---

[3] *See, e. g.,* Steve Vladeck, *Judge Bates and a FISA "Special Advocate,"* LAWFARE (Feb. 4, 2014), http://www.lawfareblog.com/2014/02/judge-batesand-a-fisa-special-advocate/ (last visited June 12, 2014); The Constitution Project, *The Case for a FISA "Special Advocate,"* (May 29, 2014), available at http://www.constitutionproject.org/wp-content/uploads/2014/05/-The–Casefor–a–FISA–Special–Advocate—FINAL.pdf. (last visited June 12, 2014). The continuity of such a position might allow the Special Advocate to recognize patterns of suspect behavior that would otherwise go unnoticed, and bring them to the court's attention before they reach the extent noted in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court, supra,* 218 F. Supp.2d at 620–21, which came to light only because the government itself informed the court after the fact.

7.

Imagining ways to make *Franks* workable in a classified setting is difficult, as the foregoing discussion demonstrates and as the government's counsel candidly acknowledged at oral argument. My purpose in engaging in this discussion has been to acknowledge a problem that thus far has not been addressed as deeply as it should be by the judiciary. Thirty-six years after the enactment of FISA, it is well past time to recognize that it is virtually impossible for a FISA defendant to make the showing that *Franks* requires in order to convene an evidentiary hearing, and that a court cannot conduct more than a limited *Franks* review on its own. Possibly there is no realistic means of reconciling *Franks* with the FISA process. But all three branches of government have an obligation to explore that question thoroughly before we rest with that conclusion.

MEMORANDUM OPINION AND ORDER OF THE DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS (JANUARY 29, 2014)

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

ADEL DAOUD,

Defendant.

No. 12 CR 723

Before: Judge Sharon Johnson COLEMAN

Defendant Adel Daoud is charged with attempting to use a weapon of mass destruction in violation of 18 U.S.C. § 2332a(a)(2)(D) and attempting to destroy a building by means of explosive in violation of 18 U.S.C. § 844(i). Daoud filed a motion for disclosure of Foreign Intelligence Surveillance Act of 1978 ("FISA") related material and to suppress the fruits or derivatives of electronic surveillance and any other means of collection conducted pursuant to FISA or other foreign intelligence gathering [51]. This Court heard oral argument on this, and other

motions, on 1/3/2014.[1] For the reasons discussed below, the motion is granted in part and denied in part.

FISA PROCEDURES

The Foreign Intelligence Surveillance Act of 1978, established detailed procedures governing the Executive Branch's ability to collect foreign intelligence information. To obtain an order authorizing electronic surveillance or physical searches of an agent of a foreign power, FISA requires the government to file under seal an *ex parte* application with the United States Foreign Intelligence Surveillance Court (the "FISC"). 50 U.S.C. §§ 1804, 1823. The application must be approved by the Attorney General and must include certain specified information. *See* 50 U.S.C. §§ 1804(a), 1823(a).

After review of the application, a single judge of the FISC will enter an *ex parte* order granting the government's application for electronic surveillance or a physical search of an agent of a foreign power, provided the judge makes certain specific findings. 50 U.S.C. §§ 1805(a), 1824(a). The FISA order must describe the target, the nature and location of the facilities or places to be searched, the information sought, and the means of acquiring such information. *See* 50 U.S.C. §§ 1805(c)(1), 1824(c)(1). The order must also set forth the period of time during which the electronic surveillance or physical searches are approved, which is generally ninety days or until the

---

[1] Unlike the Court's recent denial of discovery [87], which did not seek the discovery of classified information, the instant motion seeks disclosure of classified documents that are ordinarily not subject to discovery.

objective of the electronic surveillance or physical search has been achieved. *See* 50 U.S.C. §§ 1805(e)(1), 1824(d)(1). Applications for a renewal of the order must generally be made upon the same basis as the original application and require the same findings by the FISC. 50 U.S.C. §§ 1805(e)(2), 1824(d)(2).

The current version of FISA requires that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2006). However, FISA allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions. 50 U.S.C. §§ 1806(a), 1825(a). Here, the government provided notice, as required by FISA, of its intent to use evidence obtained and derived from electronic surveillance and physical searches pursuant to FISA orders.

FISA authorizes an "aggrieved person" to seek suppression of any evidence derived from FISA surveillance or searches either because (1) the evidence was unlawfully acquired, or (2) the electronic surveillance or physical search was not conducted in conformity with the order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). An "aggrieved person" for purposes of electronic surveillance is "a person who is the target of an electronic surveillance." 50 U.S.C. § 1801(k). For physical searches, FISA defines "aggrieved person" as "a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821.

DISCUSSION

Daoud moves for disclosure of the FISA application and materials and also moves to suppress the fruits of electronic surveillance pursuant to FISA or any other foreign intelligence information gathering. Daoud requests that this Court review all applications for electronic surveillance of the defendant pursuant to FISA; to order the disclosure of the applications for the FISA warrants to defendants' counsel pursuant to an appropriate protective order; conduct an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978); suppress all FISA intercepts and seizures, and fruits thereof, derived from illegally authorized or implemented FISA electronic surveillance; and consider the constitutionality of FISA both facially and as applied to defendant under the First and Fourth Amendment of the United States Constitution. For the reasons stated below, the motion is granted in part and denied in part.

Attorney General Eric H. Holder, Jr., filed an affidavit stating under oath that disclosure of such materials would harm national security. *See* 50 U.S.C. §§ 1806(f), 1825(g). Attorney General Holder's claim of privilege is supported by a classified declaration from an FBI official. Pursuant to FISA, the filing of an Attorney General affidavit triggers an *in camera, ex parte* procedure to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. 50 U.S.C. §§ 1806(f), 1825(g).

Once the *in camera, ex parte* procedure is triggered, the reviewing court may disclose such materials "only where such disclosure is necessary to make an accurate determination of the legality of the

surveillance." 50 U.S.C. § 1806(f); *see also* 50 U.S.C. § 1825(g). The Seventh Circuit has previously reviewed *de novo* the probable cause determination of the FISC, *United States v. Dumeisi*, 424 F.3d 526, 578 (7th Cir.2005), and therefore this Court rejects the government's request for deferential review. The factual averments and certifications used to support the government's FISA warrant application are reviewed for clear error. *United States v. Rosen*, 447 F. Supp.2d 538, 546 (D.Va.2006).

Here, counsel for defendant Daoud has stated on the record that he has top secret SCI (sensitive compartmented information) clearance. Assuming that counsel's clearances are still valid and have not expired, top secret SCI clearance would allow him to examine the classified FISA application material, if he were in the position of the Court or the prosecution. Furthermore, the government had no meaningful response to the argument by defense counsel that the supposed national security interest at stake is not implicated where defense counsel has the necessary security clearances. The government's only response at oral argument was that it has never been done. That response is unpersuasive where it is the government's claim of privilege to preserve national security that triggered this proceeding. Without a more adequate response to the question of how disclosure of materials to cleared defense counsel pursuant to protective order jeopardizes national security, this Court believes that the probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel. Upon a showing by counsel, that his clearance is still valid, this Court will allow disclosure of the FISA

application materials subject to a protective order consistent with procedures already in place to review classified materials by the court and cleared government counsel.

While this Court is mindful of the fact that no court has ever allowed disclosure of FISA materials to the defense, in this case, the Court finds that the disclosure may be necessary. This finding is not made lightly, and follows a thorough and careful review of the FISA application and related materials. The Court finds however that an accurate determination of the legality of the surveillance is best made in this case as part of an adversarial proceeding. The adversarial process is the bedrock of effective assistance of counsel protected by the Sixth Amendment. *Anders v. California*, 386 U.S. 738, 743 (1967). Indeed, though this Court is capable of making such a determination, the adversarial process is integral to safeguarding the rights of all citizens, including those charged with a crime. "The right to the effective assistance of counsel is thus the right of the accused to require the prosecution's case to survive the crucible of meaningful adversarial testing." *United States v. Cronic*, 466 U.S. 648, 656 (1984).

In sum, this Court grants disclosure to cleared defense counsel of the FISA application materials and such disclosure will be made under an appropriate protective order. By this Order, this Court does not express any opinion with respect to the constitutionality of FISA or its procedures. Nor has this Court lost sight of the potential Classified Information Procedures Act ("CIPA") issues that may be implicated by this disclosure, and resolution of those issues may result in the redaction of certain

portions of the material. Lastly, this Court denies Daoud's request to suppress all fruits of FISA surveillance without prejudice. Counsel for Daoud must present to the Court documentation of current valid security clearances at or before the next status hearing on February 6, 2014.

IT IS SO ORDERED.

/s/ Sharon Johnson Coleman
United States District Judge

Date: January 29, 2014

ORDER OF THE SEVENTH CIRCUIT DENYING PETITION FOR REHEARING EN BANC (OCTOBER 2, 2014)

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff–Appellant,

v.

ADEL DAOUD,

Defendant–Appellee.

No. 14—1284

Appeal from the United States District Court for the Northern District of Illinois, Eastern Division
No. 12 CR 723—Sharon Johnson Coleman, Judge.

Before: Richard A. POSNER, Michael S. KANNE, Ilana Diamond ROVNER, Circuit Judges.

On August 12, 2014, defendant–appellee filed a petition for rehearing *en banc*, and on September 2, 2014, plaintiff–appellant filed an answer to the petition. All the judges on the original panel have voted to deny the petition, and none of the judges in regular active service has requested a vote on the petition for rehearing *en banc*. The petition is therefore **DENIED**.

RELEVANT CONSITUTIONAL AND STATUTORY PROVISIONS

I. Constitutional Provisions

A. U.S. Const. amend. IV

The Fourth Amendment to the United States 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 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.

B. U.S. Const. amend. V

The Fifth Amendment to the United States Constitution provides, in relevant part:

> No person shall . . . be deprived of life, liberty, or property, without due process of law[.]

II. Statutory Provisions

A. 50 U.S.C. § 1806. Use of information.

(a) Compliance with minimization procedures; privileged communications; lawful purposes. Information acquired from an electronic surveillance conducted pursuant to this title [50 USCS §§ 1801 et seq.] concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only

in accordance with the minimization procedures required by this title [50 USCS §§ 1801 et seq.]. No otherwise privileged communication obtainned in accordance with, or in violation of, the provisions of this title [50 USCS §§ 1801 et seq.] shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title [50 USCS §§ 1801 et seq.] may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure. No information acquired pursuant to this title [50 USCS §§ 1801 et seq.] shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States. Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title [50 USCS §§ 1801 et seq.], the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions. Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title [50 USCS §§ 1801 et seq.], the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information

(e) Motion to suppress. Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) The information was unlawfully acquired; or

(2) The surveillance was not made in conformity with an order of author–ization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court. Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States of any State before any court or other authority of the United States or any state to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, 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. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protecttive orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion. If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders. Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information. In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines

that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination. If an emergency employment of electronic surveillance is authorized under section 105(e) [50 USCS § 1805(e)] and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) The fact of the application;

(2) The period of the surveillance; and

(3) The fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters.

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title [50 USCS §§ 1801 et seq.] may consult with

Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to co-ordinate efforts to investigate or protect against—

(A) Actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) Sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) Clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105 [50 USCS § 1805].

TRANSCRIPT OF CLASSIFIED HEARING BEFORE THE SEVENTH CIRCUIT, REDACTED (JUNE 4, 2014)

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff,

v.

ADEL DAOUD,

Defendant.

No. 14—1284

Before the Honorable Judges Richard A. POSNER, Michael S. KANNE, and Ilana Diamond ROVNER

[June 4, 2014 Transcript, p. 2]

MR. HARTENSTEIN: Yes, Your Honor, the courtroom is sealed for the protection of classified information, and the individuals in attendance are appropriately cleared.

JUDGE POSNER: Okay. Well, thank you very much. So then yes, now we have our classified hearing, and with the government's lawyers. And Judge Rovner has questions.

MR. RIDGWAY: Thank you, Judge.

JUDGE ROVNER: Let me just explain, and again, I apologize for my voice. I have a series of questions about how Daoud first came to the government's attention. I really carefully read the materials, and I fully understand that the government has taken the position that the FAA [redacted]

But because defense counsel is unable to explore this issue with you, and because this closed argument is our only opportunity to do so, I am going to pursue this area with you. So when and how did Daoud first come to the government's attention? And by Daoud I mean [redacted] And by government, I mean any branch, any agency of the United States government. Not just the FBI, not just the Justice Department, or the Chicago FBI or any of the various terms that, you know, you have used [redacted]

MR. RIDGWAY: Yes, Your Honor. [redacted]

And so you'll see information that's provided by—

JUDGE ROVNER: No, of course, I know that. But when and—when?

MR. RIDGWAY: [redacted] I would have to look at the [redacted] I know that there was

some information [redacted] But that—in terms of the source of the information, and to answer your question about the FAA, [redacted]

[redacted]

JUDGE ROVNER: If you look at page [redacted] FISA application, under the section [redacted] it states that [redacted] I'm wondering if that [redacted] is an error, because [redacted] In other words, was [redacted] under investigation by [redacted]

MR. RIDGWAY: So the—there was no—the investigation was triggered by [redacted] Now, I apologize. I used the term [redacted] earlier, and I think it should have been—

JUDGE ROVNER: [redacted]

MR. RIDGWAY: [redacted] With reference to [redacted]

JUDGE ROVNER: I knew that.

MR. RIDGWAY: Thank you. I appreciate that. And I can get the—actually I can get the application and go through that with you. [redacted]

[redacted] I can go back—I actually can go back and look at the application itself to make sure that I have got that correct if you don't mind.

JUDGE ROVNER: Sure. I'd appreciate it. Thank you.

(Brief pause.)

MR. RIDGWAY: Your Honor, I don't believe that was an error. So if I get the timeline right [redacted]

JUDGE ROVNER: [redacted]

MR. RIDGWAY: I'm sorry. Which page number are you referring to?

JUDGE ROVNER: Well, it would be the [redacted]

MR. RIDGWAY: [redacted] if I recall correctly. I'm having trouble finding where that—where, what page you're referring to, but I believe [redacted]

JUDGE ROVNER: The government's addendum at page [redacted]

MR. RIDGWAY: Oh, I'm sorry, Your Honor. I am not able to find the portion that you're referring in my materials here. It may be that I'm just not—it's not in the same order. It's government's addendum [redacted]

JUDGE ROVNER: Yes. Does the government possess—has the government ever possessed any FAA materials related to Daoud in any way?

MR. RIDGWAY: Your Honor, [redacted]

JUDGE ROVNER: Say that again, please.

MR. RIDGWAY: [redacted]

JUDGE ROVNER: Are you aware of how and when [redacted]

MR. RIDGWAY: Your Honor, I believe that information is [redacted] The—there may be [redacted] and also so I don't have additional information for that.

JUDGE ROVNER: You know, I saw that you offered to show [redacted] to the District Court. Can you provide us with access to the [redacted]

MR. RIDGWAY: Your Honor, I should be able to do that, and I say that not having been in this posture before. But we should be able to [redacted] to you.

JUDGE ROVNER: You offered them to the District Court, of course.

MR. RIDGWAY: We will work to get those as part of the record in this case.

JUDGE POSNER: Was Senator Feinstein referring to Daoud when she referenced a person who attempted to set off a car bomb in Chicago?

MR. RIDGWAY: Your Honor, I don't know whether Senator Feinstein was referring to that. It seemed—I think it seemed like in the context that it may have been a reference. I don't know what was the reason why she said that. I think in the record, though, it's clear that the counsel for the Senate has made clear that was not part of—it was not meant to be understood as a statement that the FAA was used in this case, and that the defense has been misreading those comments.

I think the more important point is that the classified record makes clear that [redacted]

JUDGE ROVNER: And only, you know, if you know [redacted] when [redacted] first received information [redacted]

MR. RIDGWAY: Your Honor, I believe that information happened [redacted] I apologize. I can—again, that would be—

JUDGE POSNER: Well, I thought your classified briefs said [redacted]

MR. RIDGWAY: In—when it comes to information [redacted]

JUDGE POSNER: From the [redacted]

MR. RIDGWAY: [redacted]

JUDGE POSNER: But that was before that, what, [redacted]

MR. RIDGWAY: It was, it was before [redacted] Obviously it—

JUDGE POSNER: Before [redacted]

MR. RIDGWAY: It was information received before the [redacted]

JUDGE ROVNER: I'm going to ask about Franks, because in Franks the Supreme Court, you know, seemed to set aside the possibility that the Court could conduct its own review of the warrant application. Do you think we should dispense with the notion that a Court could adequately conduct a real Franks review when

the Supreme Court has basically said it's not possible?

MR. RIDGWAY: I mean, no, Your Honor. Franks still applies in this setting. It just is a difficult—it's a difficult burden for, for a Franks showing to be shown—

JUDGE ROVNER: I just don't see how—

MR. RIDGWAY: —and presented.

JUDGE ROVNER: I myself don't see how it's possible. I just don't really see—

MR. RIDGWAY: Your Honor, it's very similar to the circumstances that I think in any case a defendant is always going to be making allegations about what he or she did. And to the extent those concrete allegations really give doubt about the underlying application materials, then, then that could be a circumstance in which it could be shown. I think Courts still have recognized it would be difficult. And under 22 the procedures that Congress has created in 1806(f), it would be difficult to make that showing.

Ultimately, though, that is—that was the policy judgment that Congress made in terms of the sensitivity of the information that's involved.

JUDGE ROVNER: [redacted]

MR. RIDGWAY: Your Honor, I don't know that I could give the answer to that question, [redacted] But I don't know that I can. We have submitted filings in terms of information that

with respect to the FAA, that is, if the person was an aggrieved party and that information was used in order to obtain a FISA, then that would be derived from. So I think that is spelled out in one of the filings we had with the district Court. But I don't know whether I can answer your question in terms of whether it's [redacted]

JUDGE ROVNER: And let me be sure that I understood you. [redacted]

MR. RIDGWAY: I personally do not know.

JUDGE ROVNER: You personally. Is there anyone in this room that does?

MR. RIDGWAY: I don't—I don't know that, if there is someone who would be able to answer the question differently than I have answered it.

JUDGE ROVNER: Do you want to ask them?

MR. RIDGWAY: Sure.

(Brief pause.)

MR. RIDGWAY: Your Honor, no one is able to answer the question any differently except, you know, they have reflected that for me that there, [redacted]

[redacted]

JUDGE ROVNER: And one last question. How does a person become an agent of foreign power? [redacted]

MR. RIDGWAY: Your Honor, it— [redacted]

JUDGE ROVNER: I'm very appreciative.

MR. RIDGWAY: Thank you.

JUDGE POSNER: Okay. Do you have anything?

JUDGE KANNE: No. [redacted]

MR. RIDGWAY: That's correct, Your Honor.

JUDGE KANNE: So that's the bottom line.

MR. RIDGWAY: That's the bottom line.

JUDGE POSNER: Okay. Well, thank you very much, Mr. Ridgway. And we will end our secret hearing.

MR. RIDGWAY: Thank you.