In the

United States Court of Appeals

For the Seventh Circuit

No. 14-1284

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ADEL DAOUD,

Defendant-Appellee.

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 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 acci-

---

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 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

---

dental failure to record the argument occurred in a high-profile case involving serious criminal charges.

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.*, 2014 WL 2444388, at *2 (7th Cir. June 2, 2014). And when in a criminal case the prosecutor and the defend-

ant 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*, 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 (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 (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. 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 ac-

cess 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 mo-

tion. 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.

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 9, 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 work-around.

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. 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 nonimpeachment 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 suffi-

> cient 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*, 133 S. Ct. 232 (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*, 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. 2d ___, 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. Hi. 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 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.

---

[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.

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 Amend-

ment'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 6-7. 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.*

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

---

[3] *See, e.g.*, Steve Vladeck, *Judge Bates and a FISA "Special Advocate,"* LAWFARE (Feb. 4, 2014), http://www.lawfareblog.com/2014/02/judge-bates-and-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-Case-for-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.

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.