Filed With Classified
Information Security Officer
CISO
Date 7/14/14

[redacted]

REDACTED / CLEARED FOR PUBLIC RELEASE

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

SUPPLEMENTAL CLASSIFIED OPINION DECIDED JULY 14, 2014

Before POSNER, KANNE, and ROVNER, *Circuit Judges.*

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

[redacted]

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[redacted]

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 confirming that the account belonged to a "Mr. Adel Daoud."

A few days later, an "online covert employee" of the FBI exchanged emails with and thereby obtained his IP address; on , 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]

[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]

[redacted]

[redacted]

[redacted] Cf. *Wong Sun v. United States*, 371 U.S. 471 (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.

[redacted]

[redacted]

§§ 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 (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

[redacted]

[redacted]

nongovernmental informant." *Id.* at 171. 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. [redacted]

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 [redacted] 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

[redacted]

[redacted]

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*, 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

[redacted]

[redacted]

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

[redacted]

[redacted]

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], [redacted]

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

[redacted]

[redacted]

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.

[redacted]

[redacted]

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.

[redacted]